エンタープライズ認可(Authorization)入門

NPO日本ネットワークセキュリティ協会（JNSA）
標準化部会　デジタルアイデンティティWG

2026年8月20日　発行

留意事項

本資料の作成者は、本資料の内容の正確性、安全性、有用性等について、一切の保証を与えるものではありません。また、この資料に含まれる情報および内容の利用によって、直接・間接的に生じた損害について一切の責任を負わないものとします。

本資料の使用に当たっては、以上に同意いただいた上、ご自身の責任の下ご活用いただきますようお願いいたします。

また、資料内の解説や和訳などすべての内容には、執筆者による独自の解釈を含んでいますのでご留意ください。

ご挨拶

本資料は、2024～2025年度デジタルアイデンティティWG内の「認可について考えるサブWG」にて、Identity and Access Managementの領域における「認可」とは何を指すか、各種ドキュメントを参照しつつ、約一年間にわたって検討した内容をまとめたものです。

読者は日本の企業や組織において業務に利用されるシステムやITサービスの、セキュリティ管理者やITリスク管理者、Enterprise Architecture担当、社内システム共通基盤担当部門の方々を想定しています。

読者の方が「認可」に関連して社内あるいは社外とコミュニケーションをとる際に、本書が関係者の共通理解を助け、コミュニケーションのハードルを下げることに少しでも寄与出来ましたら幸いです。

本資料の作成にあたり、作成メンバーにご尽力いただいたことに、この場を借りて謝辞申し上げます。

標準化部会　デジタルアイデンティティWGリーダー　貞弘　崇行

目次

1. はじめに
2. 認可とは
   - ✓ 既出定義の確認
   - ✓ 本資料における定義
3. 認可の定義から見る関連用語や概念
   - ✓ アクセス制御モデルの整理（IBAC）
   - ✓ アクセス制御モデルの整理（RBAC）
   - ✓ アクセス制御モデルの整理（ABAC）
4. 認可を実現する論理モデル（PxP）
5. システム利用における認可制御

- ✓ Appendix A. OAuth2での認可との違いは？
- ✓ Appendix B. ロール管理とは

1. はじめに

背景

- ✓ 企業・組織において重要なデジタル資産(情報・システム)を守るために、アイデンティティ・認証・認可を適切に管理することが重要であることは誰もが理解している。このうち、アイデンティティの管理・認証については、各種ガイドラインの普及や定義の統一、標準化の発展とともに、多くの企業・組織がIDaaSによるユーザ情報の一元管理やMFAなどによる認証強度の向上など、成熟度を高めている。
- ✓ 一方で、デジタル資産を守る最後の砦である認可については、管理の方式が千差万別であり、各システムに任せきりになっており、適切な管理ができているかどうかが確認できない状態である企業が多い。
- ✓ 最小権限の原則を徹底するために、認可についてもよりステップアップしていく必要がある。
- ✓ 認可については用語やモデルが統一されていないため、同じ言葉が複数の意味を持っていることも多く、検討時のコミュニケーションにおいて誤解が生じやすい。

目的・ねらい・対象想定読者

- ✓ 目的・ねらい
  - ✓ 日本の企業・組織における認可管理の高度化を促進する
  - ✓ 認可に関する用語・概念を整理し、共通理解を助け、認可の高度化にむけたコミュニケーションのハードルを下げる。
- ✓ スコープ
  - ✓ 企業・組織において業務に利用されるシステム・ITサービス
- ✓ 想定読者
  - ✓ セキュリティ管理者・ITリスク管理者
  - ✓ Enterprise Architecture担当、社内システム共通基盤担当部門

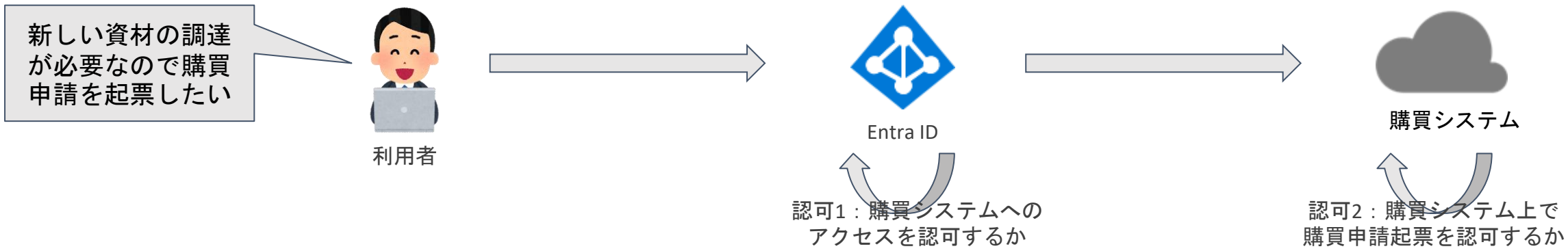
認可の例と本資料の構成

デジタル資産を守る最後の砦である認可だが、適切な認可を実現するためには適切な箇所で適切な考え方に基づいた認可を実施する必要がある。例えば、ある利用者がEntra IDで保護されている購買システムにアクセスして購買申請を起票するケースを考えてみる。

このケースでは以下2箇所での認可を通して、購買申請の起票を認可したと考えられる。

認可1（Entra IDにて）：利用者の所属部署やアクセス状況（場所など）に基づく購買システムへのアクセスの認可*

認可2（購買システムにて）：業務上の役割に基づく購買システム上で購買申請起票の認可



本資料では、まず「2. 認可とは」にて認可の定義を整理する。上述の認可1や認可2で用いられることが多いロールや属性に基づくアクセス制御などの考え方については、本資料「3.関連用語や概念との関係」で整理している。さらに、適切な認可を行うために必要なコンポーネントとそこでの考え方の組み合わせ方は、本資料「4. 認可を実現する論理モデル（PxP）」、「5. システム利用における認可制御」で整理している。

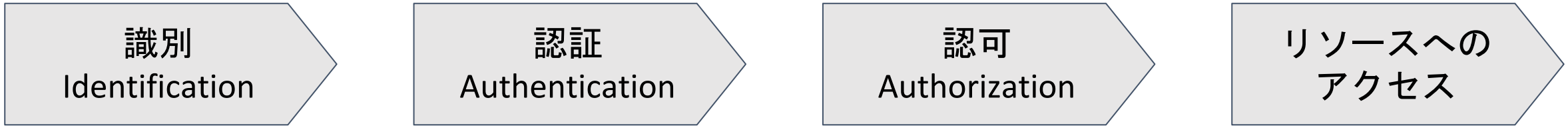
*：Entra IDは、利用者の認証を行った後に認証連携先へのアクセスを認可する。ここでは、この認可を指す。

2. 認可とは

2. 認可とは
- 既出定義の確認

リソースへのアクセスに至るまでのプロセス

- ✓ 認可とはある主体がリソースへのアクセスに至るまでに必要なプロセスの一つであることは広く受け入れられている（例 NIST 800-53 Revision 5）。
- ✓ リソースへのアクセスまでには、識別・認証・認可のプロセスが必要であり、認可はそのプロセスの一つと位置付けられる。



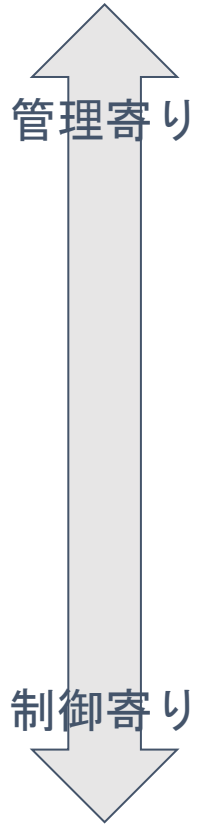
各プロセスの定義

- ✓ 識別、認証、認可の各プロセスの定義を確認すると、識別や認証については下表に示す定義の統一・周知が進んでいるように見える。
- ✓ 一方、認可の定義については、定義の統一は不十分と考えられる。

#	プロセス	定義	出典
1	識別	The process of discovering the identity (i.e., origin or initial history) of a person or item from the entire collection of similar persons or items. 同様の人やモノの集合から、特定の人やモノのアイデンティティを見分けるプロセス	FIPS201-3
2	認証	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources. （よくあるケースとしてはシステムのリソースへのアクセスを許可する前提条件として、）人、プロセス、デバイスのアイデンティティを検証すること	NIST800-63-3
3	認可	ガイドによって定義が様々。次頁参照。	次頁参照

ガイドごとの認可の定義

#	プロセス	定義	出典
3-1	認可	The official management decision given by a senior organizational official to authorize the operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security controls 事前合意されたセキュリティコントロールの実装に基づき、情報システムの運用を認可し、国家、他の組織、個人、資産、組織運用に対するリスクを明示的に許容することの組織幹部による正式な管理上の判断	NIST 800-175: Guideline for Using Cryptographic Standards in the Federal Government
3-2		Access privileges granted to a user, program, or process or the act of granting those privileges. 利用者やプログラム、プロセスに与えられたアクセス権もしくはアクセス権付与すること	NIST SP800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations
3-3		ポリシーとの照合による評価に基づいてアクセスを許可するか決定し、その結果を発行・通知する処理。	DS-212: ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート
3-4		The process of verifying that a requested action or service is approved for a specific entity. アクションやサービスへのリクエストが特定の主体に対して許可されているかを検証するプロセス	NIST SP800-152: A Profile for U.S. Federal Cryptographic Key Management Systems



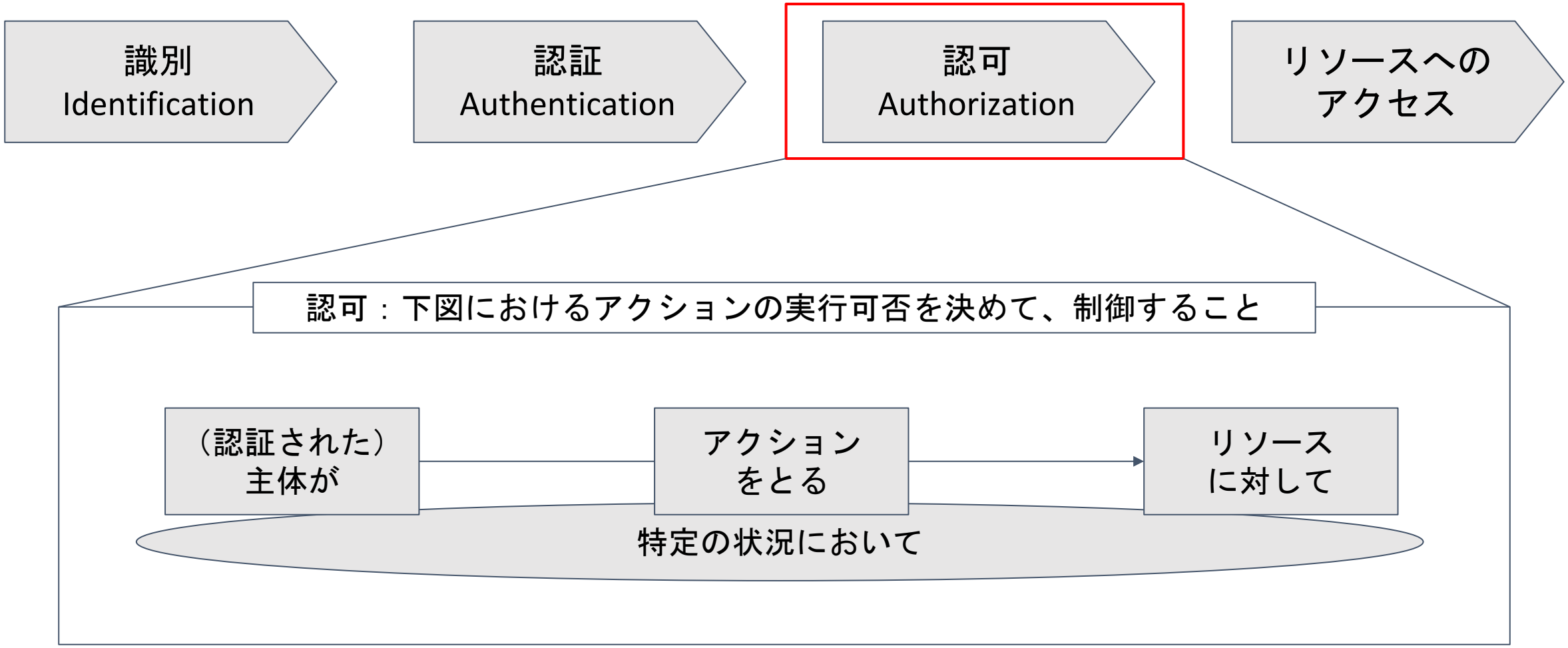
2. 認可とは
- 本資料における定義

認可とは（本資料における定義）

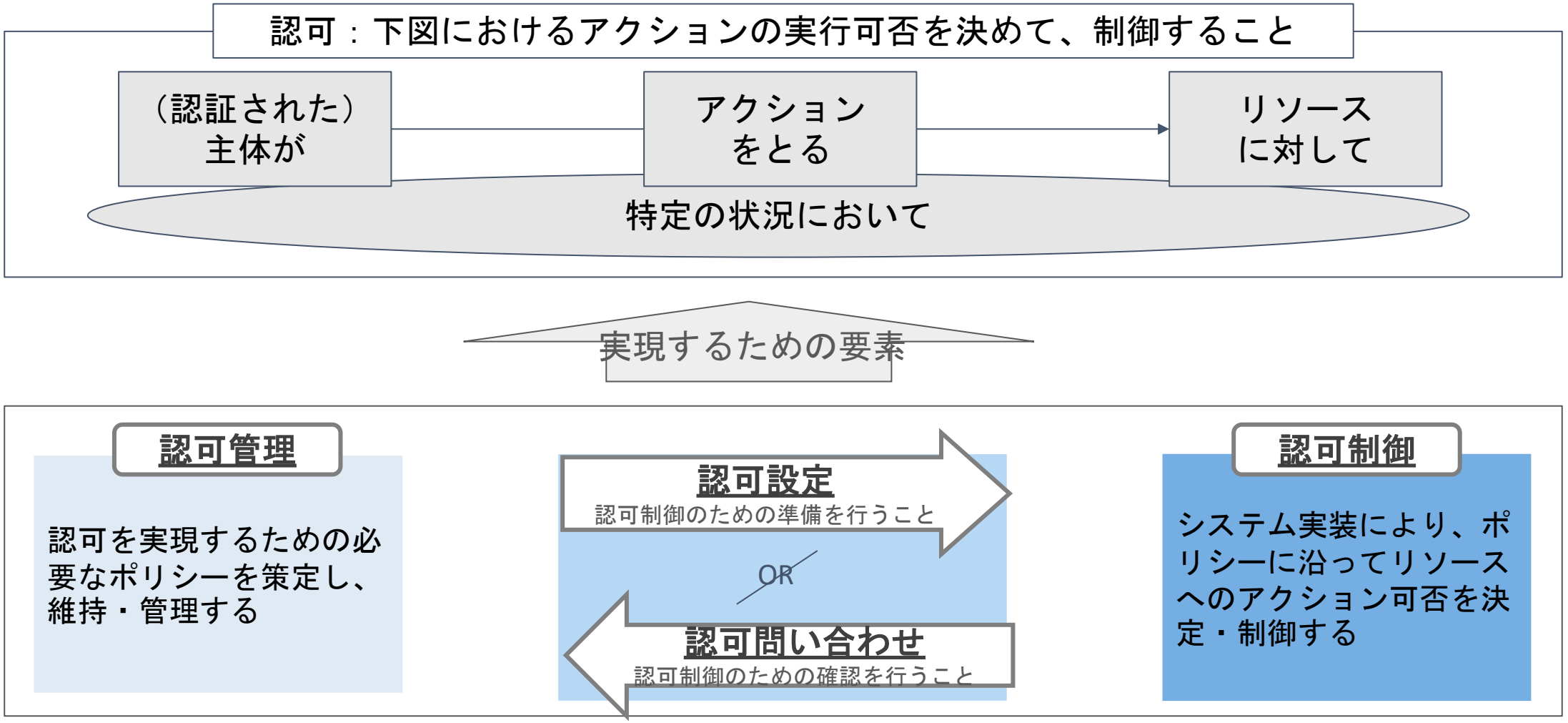
- ✓ 各ガイドラインでの認可の定義を整理すると、認可には以下2つの側面があると理解できる。
  - ✓ リソースへのアクセスを許可すべきかのポリシー*1（アクセス制御ポリシー）策定とその維持・管理
  - ✓ そのポリシーに基づくリソースへのアクセス可否の制御
- ✓ 本資料では、上記を踏まえ、認可の定義を次の通りとする。
  - ✓ **特定の主体が、特定のリソースに対して、特定の状況において、特定のアクションを実行する際に、その実行可否をポリシー*1に基づいて決定し、その通りに制御すること。**
    - ✓ なお、この実行可否を決めるためのポリシーは、認可管理*2において策定され、維持・管理される。実システム上での実行可否は認可制御*2において決定され、制御される。
- ✓ この定義を図示すると次頁の通り。

*1 ポリシーとは、主体について正しい、あるいは、期待される振る舞いを特定する声明、ルール、主張（NIST 800-95）
*2 認可管理および認可制御については2ページ先の図を参照

認可とは（図示）1/2



認可とは（図示）2/2



3. 認可の定義から見る関連用語や概念

認可の定義に沿って整理する関連用語や概念

- ✓ 前述の定義とその構成要素に沿って、認可に関連して頻出する用語や概念を整理することが可能と考える。
- ✓ 本章では、アクセス制御モデル（Xベースアクセス制御）に基づく用語や概念を取り上げて整理を試みる。
  - ✓ アイデンティティベースアクセス制御
  - ✓ ロールベースアクセス制御
  - ✓ 属性ベースアクセス制御
- ✓ OAuth2における「認可」との違いについても本資料のAppendix Aに記載があるので、参考にされたし。

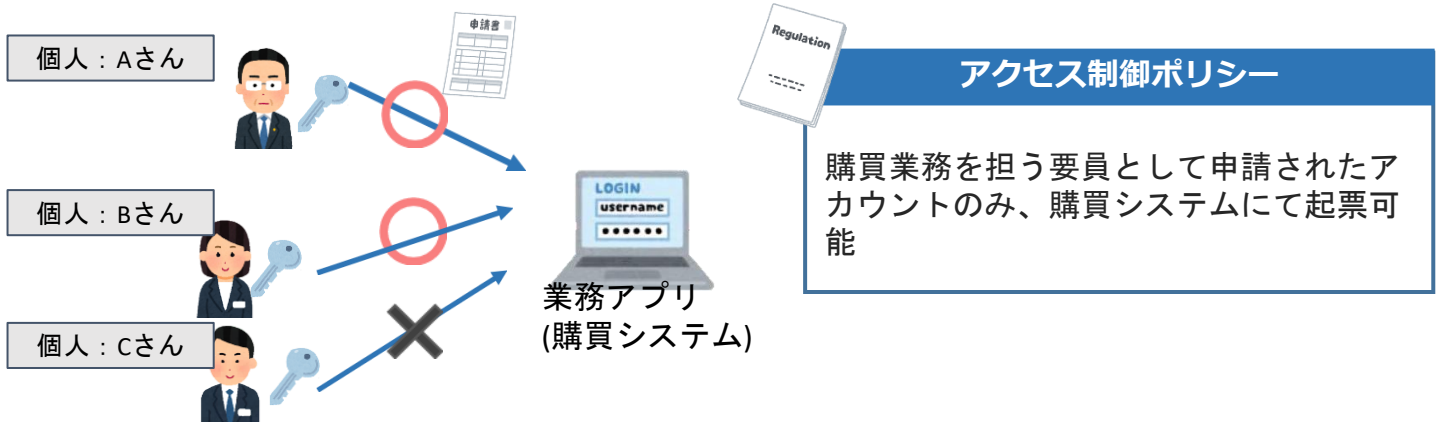
3. 認可の定義から見る関連用語や概念
- アクセス制御モデルの整理（IBAC）

アクセス制御モデルの整理（IBAC） 1/4

アクセス制御モデル	説明	URL / ソース
アイデンティティベースアクセス制御（以下IBAC）	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. ユーザーのアイデンティティに基づくアクセス制御（通常、そのユーザーの代理を務めるプロセスの特性として中継される）ここで、特定のオブジェクトへのアクセス権限は、ユーザーIDに基づいて割り当てられる。	https://csrc.nist.gov/glossary/term/identity_based_access_control CNSSI 4009-2015

アクセス制御モデルの整理（IBAC） 2/4

例	購買業務を担う個人には購買システム上での購買申請の起票可能権限を割り当てる。対象の個人は以下。 ・購買業務を担うAさん ・購買業務を担うBさん



アクセス制御モデルの整理（IBAC） 3/4

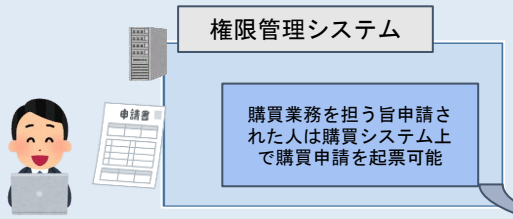
	認可管理	認可設定	認可制御
IBACで必要な認可管理と認可制御	主体とリソースの間に、必要な関係を定義・管理	定義された関係を使って制御できるよう準備	主体とリソースの関係を評価し、アクセス可否を制御
IBACの具体例：購買システム上での購買申請起票可否制御	購買業務を担う人は、購買システム上で購買申請起票が可能とするポリシーを定義	購買業務を担う旨の申請に基づき、購買システムで、Aさんを申請起票可能と設定	購買システムは、ポリシーに基づいてAさんによる起票操作を許可する。

アクセス制御モデルの整理（IBAC） 4/4

IBACの具体例：購買システム上での購買申請起票の可否制御イメージ

認可管理

購買業務を担う人は、購買システム上で購買申請起票が可能とするポリシーを定義



認可設定

購買業務を担う旨の申請に基づき、購買システムで、Aさんを申請起票可能と設定

管理者がAさんを購買申請起票可能に設定

認可制御

購買システムは、設定に基づいてAさんによる起票操作を許可する。

3. 認可の定義から見る関連用語や概念
- アクセス制御モデルの整理（RBAC）

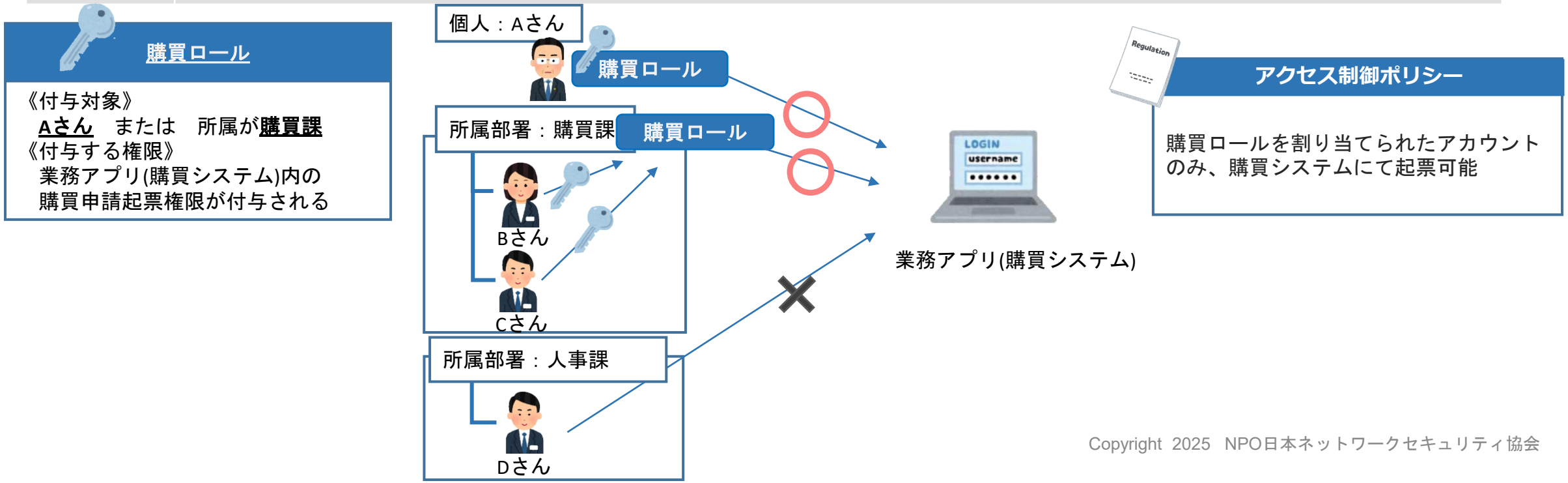
アクセス制御モデルの整理（RBAC） 1/4

アクセス制御モデル	説明	URL / ソース
ロールベースアクセス制御 （以下RBAC）	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. ユーザーのロールに基づくアクセス制御（すなわち、与えられたロール（役割）の明示的または暗黙的な仮定に基づいて、ユーザーが受け取るアクセス権限のコレクション）。ロール*の権限は、ロール*の階層を通じて継承されることがあり、通常、組織内で定義された機能を実行するために必要な権限を反映する。与えられたロール*は、一人の個人に適用されることもあれば、複数の個人に適用されることもある。	https://csrc.nist.gov/glossary/term/role_based_access_control CNSSI 4009-2015 NIST SP 800-53 Rev. 5

*：ロールを使ったアクセス制御を行う際にはロール管理が必要になる。ロール管理の意義を含むロール管理概要については、Appendix Bを参照。

アクセス制御モデルの整理（RBAC） 2/4

例	購買業務を担う個人あるいは組織には購買ロールを割り当てる。対象の個人及び組織は以下。 ・特例として申請が承認されたAさん ・購買業務を担う購買課 購買ロールを割り当てられた場合は、以下システム内で購買申請を起票できる権限を付与される。 ・購買システム ・など



アクセス制御モデルの整理（RBAC） 3/4

	認可管理	認可設定	認可制御
RBACで必要な認可管理と認可制御	主体とロール、ロールとリソースの間に、必要な関係を定義・管理	定義された関係を使って制御できるよう準備	リソースとロールの関係を評価し、アクセス可否を制御
RBACの具体例：購買システムへの購買申請起票可否制御	所属が「購買課」に「購買ロール」を付与。 購買ロールが付与された人は、業務アプリ(購買システム)内の**購買申請起票可とする**ポリシーを定義	人事情報に基づき、アカウント管理システムが、AD上のBさんアカウントを「購買ロール」セキュリティグループにメンバー追加	業務アプリ(購買システム)は、ADのセキュリティグループのメンバーシップに基づいて購買申請起票制御を行う。 アクセスしたアカウント(Bさん)が「購買ロール」セキュリティグループのメンバーであるため、購買申請起票を許可する。

アクセス制御モデルの整理（RBAC） 4/4

RBACの具体例：購買システム上での購買申請起票の可否制御イメージ

認可管理

所属が「購買課」に「購買ロール」を付与。
購買ロールが付与された人は、業務アプリ(購買システム)内の**購買申請起票権限可とする**ポリシーを定義

ロール管理システム

購買ロール

《付与対象》
所属が **購買課**
《付与する権限》
業務アプリ(購買システム)内の
購買申請起票権限が付与される

認可設定

人事情報に基づき、アカウント管理システムが、AD上のBさんアカウントを「購買ロール」セキュリティグループにメンバー追加

アカウント管理システム

Active Directory

User

Bさん
所属：購買課

メンバ追加

Group

購買ロール

認可制御

業務アプリ(購買システム)は、ADのセキュリティグループのメンバーシップに基づいて購買申請起票制御を行う。
アクセスしたアカウント(Bさん)が「購買ロール」セキュリティグループのメンバーであるため、購買申請起票権限を許可する。

データ
アクセス

Bさん

LOGIN
username

業務アプリ
(購買システム)

「購買ロール」を保持しているため、データ編集可

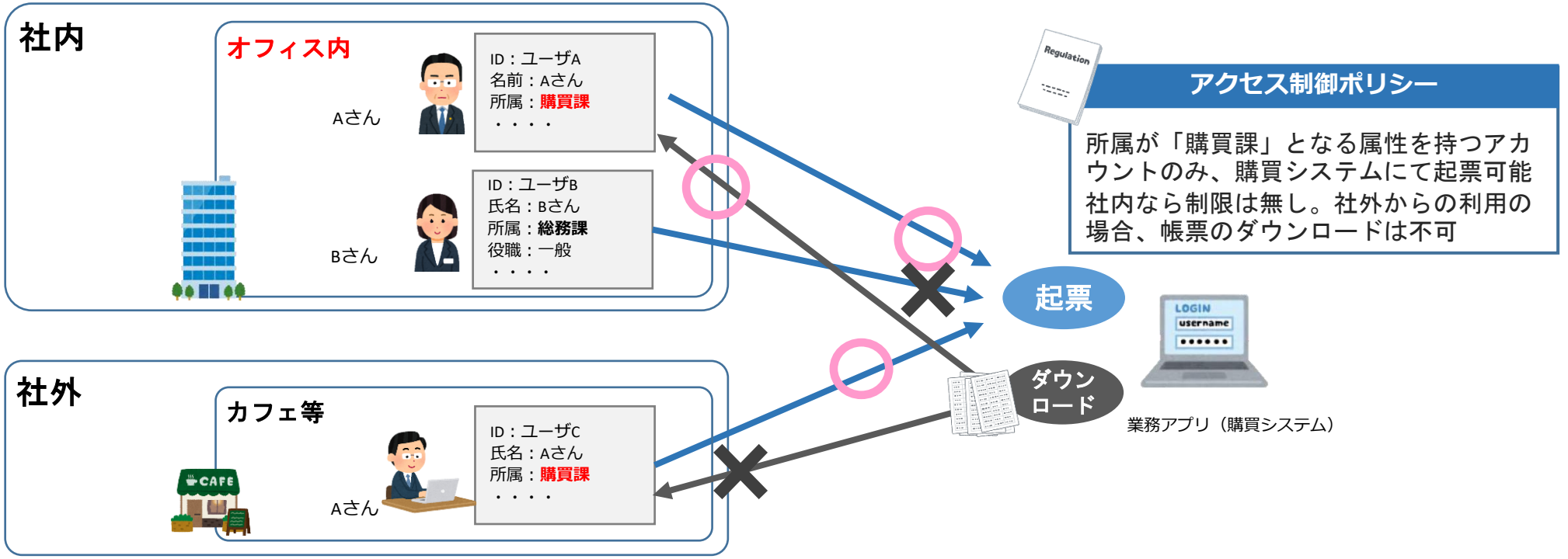
3. 認可の定義から見る関連用語や概念
- アクセス制御モデルの整理（ABAC）

アクセス制御モデルの整理（ABAC） 1/5

アクセス制御モデル	説明	URL / ソース
属性ベースアクセス制御 （以下ABAC）	Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. アクセス制御（Access Control） 主体、オブジェクト、ターゲット、イニシエータ、リソース、または環境に関連する属性に基づくアクセス制御。アクセス制御規則セットは、アクセスを行うことができる属性の組み合わせを定義する。	https://csrc.nist.gov/glossary/term/attribute_based_access_control CNSSI 4009-2015 NIST SP 800-53 Rev. 5

アクセス制御モデルの整理（ABAC） 2/5

例	購買システムでの権限管理は以下とする ・購買課のユーザは購買申請を起票可能 ・社内からの利用の場合、購買課ユーザは帳票のダウンロードが可能 ・社外からのアクセスの場合、帳票のダウンロードは不可



アクセス制御モデルの整理（ABAC） 3/5

	認可管理	認可設定	認可制御
ABACで必要な認可管理と認可制御	主体の属性や環境に関連する属性などとリソースとの間に、必要な相関関係を定義・管理	定義された関係を使って制御できるよう準備	主体の属性や環境に関連する属性などを評価し、その相関関係に基づき、アクセス可否を制御
ABACの具体例：購買システムへの購買申請起票可否および帳票のダウンロード可否制御	所属が「購買課」となる人のみ、購買システムにて購買申請を起票可能	人事担当は、異動に伴いAさんの所属を「購買課」に設定 アカウント管理システムがADに対してAさんの情報を連携する	購買システムはアクセスしたアカウント(Aさん)のAD上の属性を取得し、その所属属性が「購買課」であれば起票を許可する
	社内なら制限は無し。社外からの利用の場合、帳票のダウンロードは不可	購買システムにてリバースプロキシからのアクセスの場合は、ダウンロードメニューを非表示とするように設定	購買システムは接続元のIPアドレスをチェックし、リバースプロキシのIPアドレスとなっている場合は、ダウンロードメニューの表示を禁止

アクセス制御モデルの整理（ABAC） 4/5

ABACの具体例：購買システム上での購買申請起票の可否制御イメージ

認可管理

所属が「購買課」となる属性を持つアカウントのみ、購買システムにて起票可能

社内なら制限は無し。社外からの利用の場合、帳票のダウンロードは不可

アクセス制御ポリシー

所属が「購買課」となる属性を持つアカウントのみ、購買システムにて起票可能

社内なら制限は無し。社外からの利用の場合、帳票のダウンロードは不可

認可設定

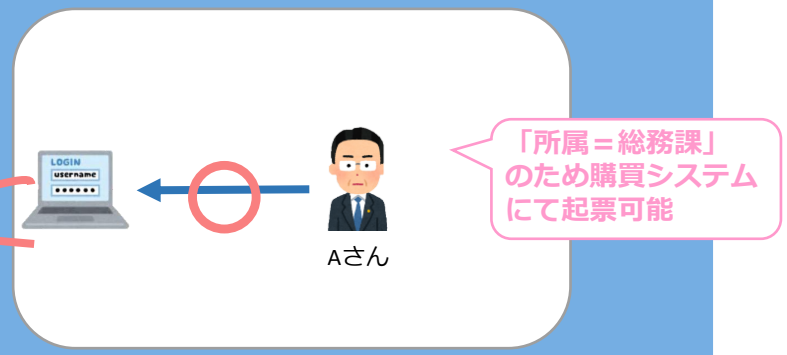
人事担当は、異動に伴いAさんの所属を「購買課」に設定
アカウント管理システムが購買システムに対してAさんの情報を連携する

購買システムにてダウンロード権限を設定
リバースプロキシからのアクセスの場合は、ダウンロードメニューを非表示とするように設定

認可制御

購買システムはアクセスしたアカウント(Aさん)のAD上の属性を取得し、その所属属性が「購買課」であれば起票を許可する

購買システムは接続元のIPアドレスをチェックし、リバースプロキシのIPアドレスとなっている場合は、ダウンロードメニューの表示を禁止



アクセス制御モデルの整理（ABAC） 5/5

ABACの具体例：購買システム上での帳票のダウンロード可否制御イメージ

認可管理

所属が「購買課」となる属性を持つアカウントのみ、購買システムにて起票可能

社内なら制限は無し。社外からの利用の場合、帳票のダウンロードは不可

アクセス制御ポリシー

所属が「購買課」となる属性を持つアカウントのみ、購買システムにて起票可能
社内なら制限は無し。社外からの利用の場合、帳票のダウンロードは不可

認可設定

人事担当は、異動に伴いAさんの所属を「購買課」に設定
アカウント管理システムが購買システムに対してAさんの情報を連携する

購買システムにてダウンロード権限を設定
リバースプロキシからのアクセスの場合は、ダウンロードメニューを非表示とするように設定

アカウント管理システム

購買システム

属性情報のセット

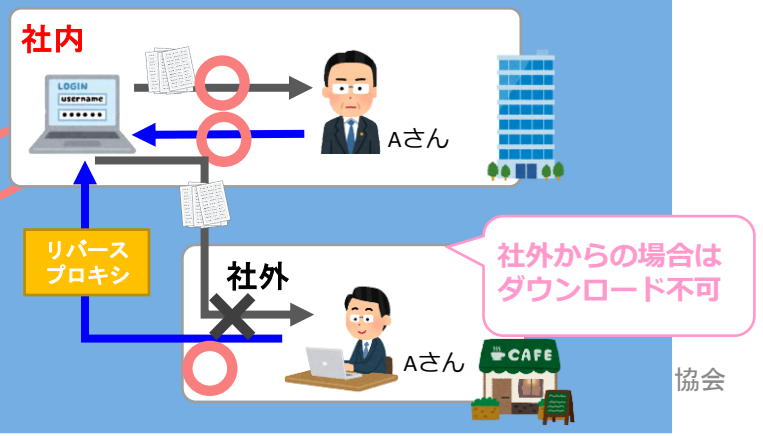
ユーザ名	名前	所属
ユーザA	Aさん	購買課
ユーザB	Bさん	総務課

メニュー権限	場所	所属
ダウンロード	社内のみ	購買課
起票	社内／社外	購買課

認可制御

購買システムはアクセスしたアカウント(Aさん)のAD上の属性を取得し、その所属属性が「購買課」であれば起票を許可する

購買システムは接続元のIPアドレスをチェックし、リバースプロキシのIPアドレスとなっている場合は、ダウンロードメニューの表示を禁止



アクセス制御モデルの整理 まとめ 1/2

本資料における認可の定義とその構成要素に沿って、各アクセス制御モデルを整理すると、各アクセス制御モデルは、本資料における認可を構成する以下の要素すべてを含むモデルであることがわかる。

- 認可管理
- 認可設定（認可問い合わせ）
- 認可制御

これまで見てきた通り、各アクセス制御モデルは上記の構成要素に組み入れられる要素が異なっており、その結果、各アクセス制御モデルごとの認可時に組み入れられる要素の違いを生んでいる。この違いが各アクセス制御モデルの特徴となる。

アクセス制御モデルの整理 まとめ 2/2

各アクセス制御モデルにおける認可時に組み入れられる要素の差をまとめると下表の通り。

アクセス制御モデル	認可時に組み入れられる要素					
	主体		実施アクション	コンテキスト	リソース	
	動的属性	静的属性			動的属性	静的属性
	例　主体のアクセス元、利用デバイス、認証強度	例　主体の役職、所属組織	例　読み取り、書き込み	例　日時	例　リソースのパッチ適用状況	例　リソースの機密レベル
IBAC	×	× （識別子のみ）	○	×	×	×
RBAC	×	○ （ロール）	○	×	×	○
ABAC	○	○	○	○	○	○

4. 認可を実現する論理モデル（PxP）

認可における論理モデルのPxPとは

システムにおいては、様々なコンポーネントを用いて、システムに対する認可を実現している。この認可を実現するにあたり、PxPと呼ばれる論理モデルを利用することで、各コンポーネントの役割を明確にし、整合性のとれた環境を実現することができる。

上述の通り、PxPとは認可を実現するための論理モデルであり、「PDP」や「PIP」など、中央の「x」部分に異なる役割をもつコンポーネントを当てはめることで、認可の概念を整理、記述することができる。

主には、eXtensible Access Control Markup Language（以下、XACML）と呼ばれるアクセス制御を実現するためのポリシー記述言語や、NIST SP800-162（属性ベースアクセス制御に関するガイドライン）において記載がされている概念であり、PxPを理解することは、セキュアかつ拡張性を有した認可制御の設計、実装に向けて有用な要素と言える。

PxPに関連する用語定義

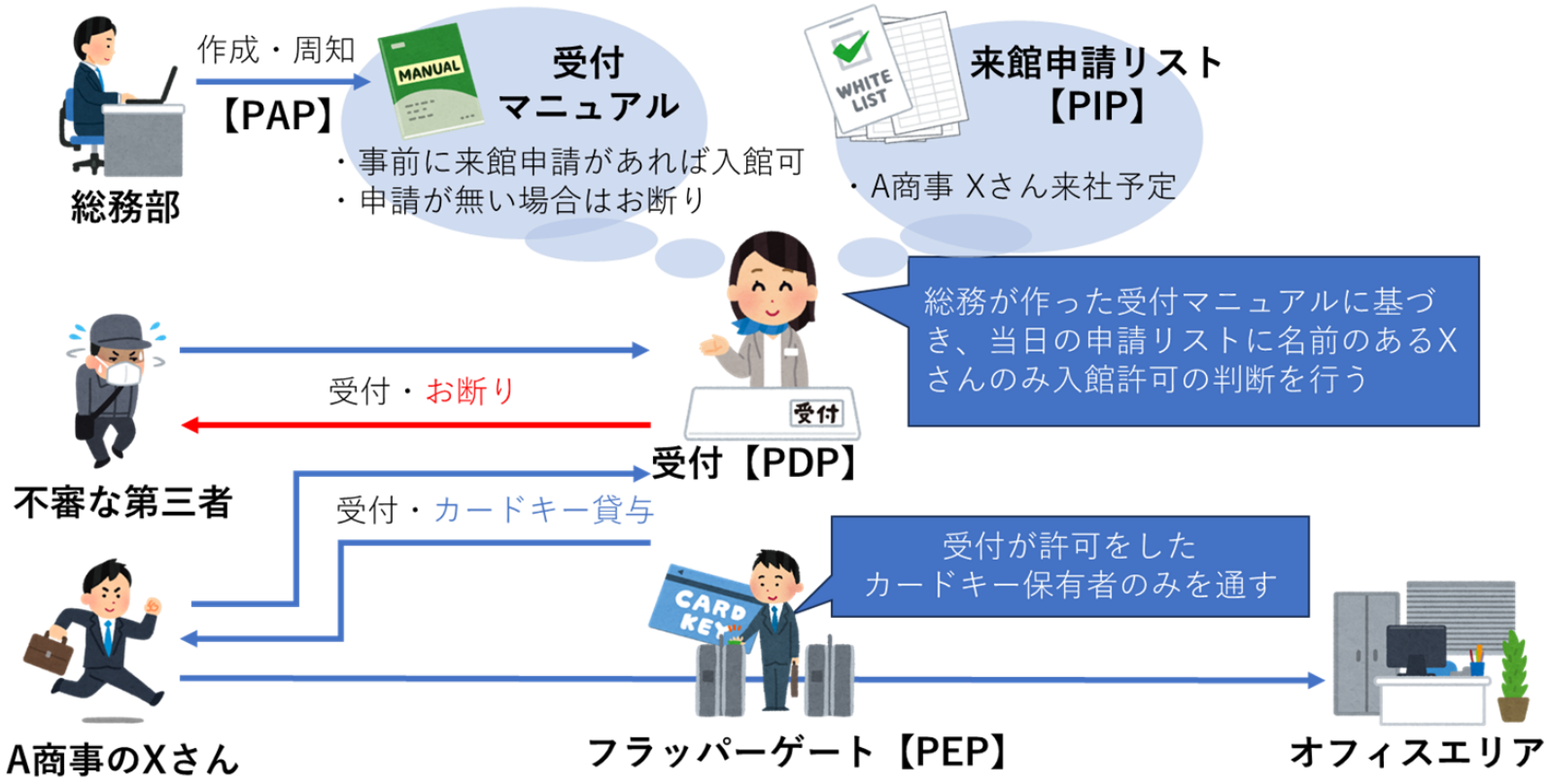
PxPに関連する用語においては、複数のドキュメントにてそれぞれの定義が記載されているが、各ドキュメントの内容によってニュアンスが異なる使われ方がされている。そのため本資料では、各ドキュメントの内容を踏まえ、以下の適宜として取り扱うこととする。

用語	説明
PxP	アクセス制御のための一連のコンポーネントであり、ポリシーの定義、検証、適用のプロセスをサポートするための仕組みを本資料では「PxP」と総称している。PxPの「x」部分に各構成要素を当てはめ、それぞれを連携して動作させることで組織のアクセス制御を効率的かつセキュアに実現する。
Policy Decision Point （以下、PDP）	リクエストされたアクション（誰が、何に対して、どのような操作をするのか）に基づいて、事前に定義されたアクセス制御ポリシーを評価するコンポーネント。リクエストされたアクションを、許可するか拒否するか決定する。 ※SP800-207ではPDP内の主体としてPolicy Engine（以下、PE）とPolicy Administrator（以下、PA）の2つのコンポーネントが定義されている PE⇒リソースへのアクセスの許可・拒否を行う際、判断ロジックとしての機能を担う。判断結果をログに残し、この情報をPAで処理する。 PA⇒アクセス主体とリソース間の通信経路の確立や遮断を行う。(認証トークンやクレデンシャル)
Policy Enforcement Point （以下、PEP）	PDPによって決定された結果に基づいて、実際の処理（アクセスの許可または拒否）を行うコンポーネント。
Policy Administration Point （以下、PAP）	PDPが参照するアクセス制御ポリシーを定義（作成、変更、削除等の管理）するためのコンポーネント。
Policy Information Point （以下、PIP）	PDPに記載されているリクエストされたアクションを評価するためのアクセス制御ポリシー情報を保存し、PDPからの問合せに応答するコンポーネント。

参考文献：NIST SP800-162, NIST SP800-207, SP1800-35

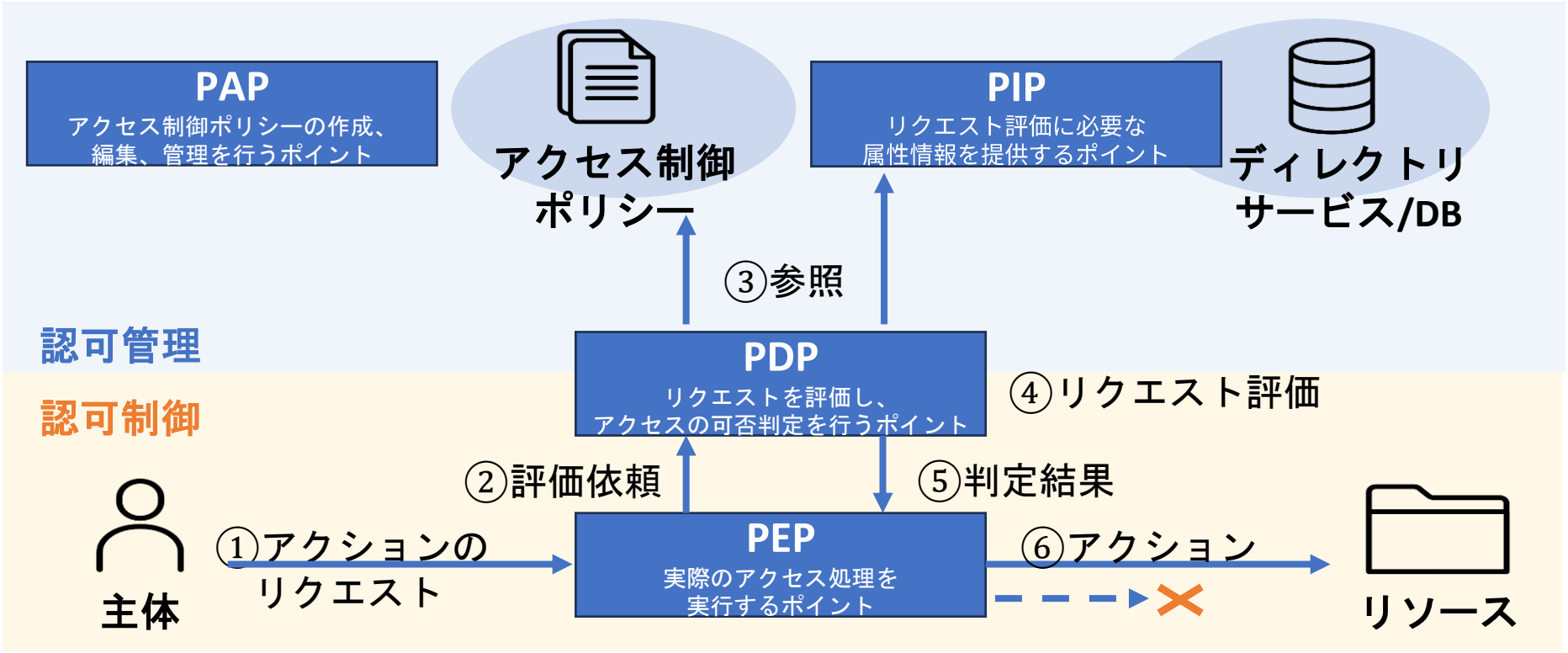
アナログ世界における認可との対比

「認可」の論理モデルと聞くとハードルが高くとも、アナログ世界にも同じ概念は存在する。
例えば来社対応を想像した時、受付担当者は訪問者をフラッパーゲートを通す（認可）かの判断を、訪問者の身元情報（認証）を確認した上で、事前に取り決めた受付マニュアル（アクセス制御ポリシー）に照らし合わせながら判断している。



PxP論理モデル

前述したPxPの各用語について、図示したものが以下の通り。
アクセス元（主体）からリクエスト先（リソース）へのアクセス（アクション）に適正なコントロールを適用するためには、各PxPのコンポーネントによりアクセスの可否判定および判定結果に基づくアクセス処理を行う必要がある。



アクセス制御の流れ

①主体がアクション（閲覧や編集等）をリクエスト

②リクエスト内容の諾否について評価を依頼

③事前に取り決めたアクセス制御ポリシーを参照

④参照結果を基に、リクエストの許可または拒否を判定

⑤判定結果を回答

⑥判定結果に基づき、主体からリソースに対するアクションへのコントロールを適用

5. システム利用における認可制御

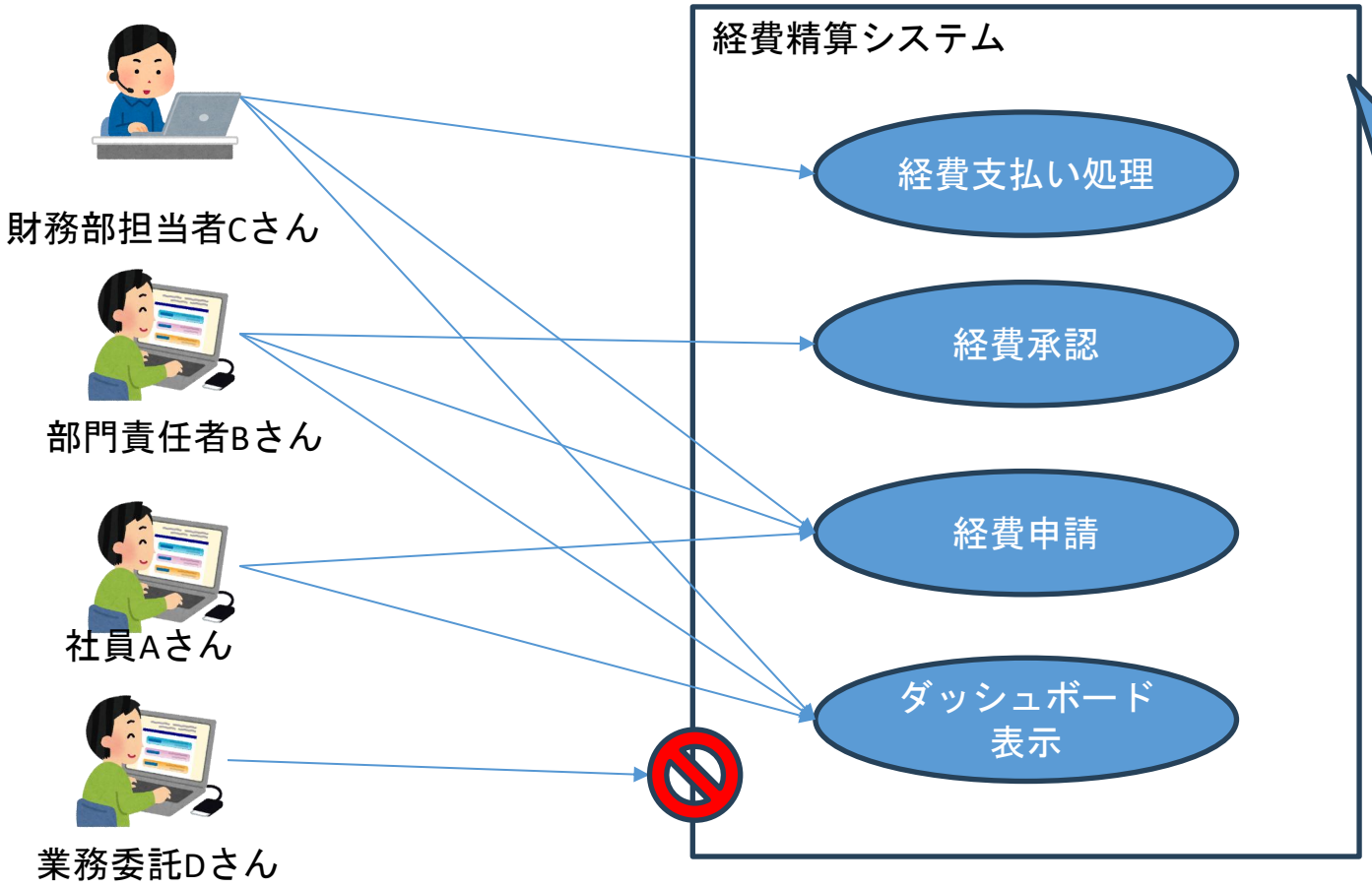
システム利用における認可制御

システムの利用においては、ユーザーの立場や役割によって、様々な操作を行うことが想定される。また、各種操作においては、複数のステップ（ログイン、メニュー選択、各種操作等）を経てシステムに対するアクションを実施するが、この一連の操作の各ステップにおいても、対象ユーザーが適切な権限を持っているのか、適切な条件を満たしているのかといった認可の制御が実装されている。

本章では、こういったシステム利用のユースケースを踏まえ、各システム上でどういった認可制御が実施されているのか、またその制御の中でPxPの論理モデルをどう適用すべきなのかを整理する。

システム利用における認可制御

ユーザーに対して各種サービスを提供するシステム考えた場合に、システム上の各種操作に対する認可の処理を検討する必要がある。以下の図では、一例として経費精算システムを例示する。この経費精算システムにおいては、ユーザーの立場や実施する操作に対して適切な認可制御を実現する必要がある。



例）経費精算システムのアクセス制御ポリシー

- 経費精算システムにアクセスできるのは社員のみ
- 社員は、自身に関連する経費の精算を行うことができる
- 部門責任者は自身の管理する部下からの経費申請を承認することができる
- 財務部担当者は、社内ネットワークからのアクセスに限り、承認された経費申請に基づき、各種支払処理を実行が可能

経費申請するケースにおける認可制御

ユーザーが経費申請するケースにおいては、下図に示す通り、経費申請が完了するまでに、経費精算システムへのログイン、ダッシュボードからのメニューの選択、など、ユーザーである主体は複数のアクションを操作として実行する。

こうした各操作において、主体が必要とする権限は何か、権限以外に満たすべき条件は何か、を定めたポリシーに沿った認可の実現が必要である。

たとえば、経費精算のステップでは、社員であるということが認可の条件となっているため、ユーザーの社員区分に応じた制御（RBAC）が適用されている。

ユースケース①　社員が経費申請をする場合の認可のステップ

アクセス開始

経費精算システムにログインし、経費情報を入力し申請する

申請完了

経費精算システムにログイン

対象ユーザーの資格情報を確認したうえで、**社員である場合にはアクセスを許可**する

ダッシュボードの表示

社員である場合には、経費申請メニューを表示

経費申請

社員からの、**自身に関連する経費精算であれば、申請を許可**する

経費承認するケースにおける認可制御

ユーザーが経費申請するケースにおいては、下図に示す通り、経費申請が完了するまでに、経費精算システムへのログイン、ダッシュボードからのメニューの選択、など、ユーザーである主体は複数のアクションを操作として実行する。

こうした各操作において、主体が必要とする権限は何か、権限以外に満たすべき条件は何か、を定めたポリシーに沿った認可の実現が必要である。

経費承認のステップでは、システムログインに関しては、社員であるということが認可の条件となっているが、経費承認メニューの表示、経費の承認といった操作には、部門管理者であるという、ユーザーの社員区分に応じた制御（RBAC）が適用されている。

ユースケース②　部門管理者が経費承認をする場合の認可のステップ

アクセス開始

経費精算システムにログインし、自分の部下の経費申請情報を確認し、申請を承認する

承認完了

経費精算システムにログイン

対象ユーザーの資格情報を確認したうえで、**社員である場合にはアクセスを許可**する

ダッシュボードの表示

部門管理者である場合には、経費承認メニューを表示

経費承認

部門管理者である場合には、**部下の経費申請一覧を表示し、承認を許可**する

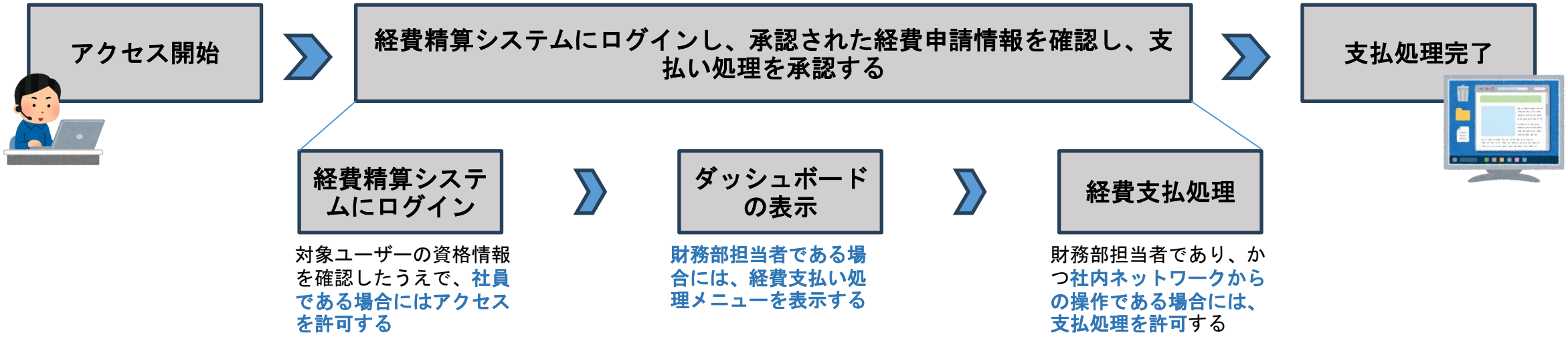
経費の支払実施するケースにおける認可制御

ユーザーが経費申請するケースにおいては、下図に示す通り、経費申請が完了するまでに、経費精算システムへのログイン、ダッシュボードからのメニューの選択、など、ユーザーである主体は複数のアクションを操作として実行する。

こうした各操作において、主体が必要とする権限は何か、権限以外に満たすべき条件は何か、を定めたポリシーに沿った認可の実現が必要である。

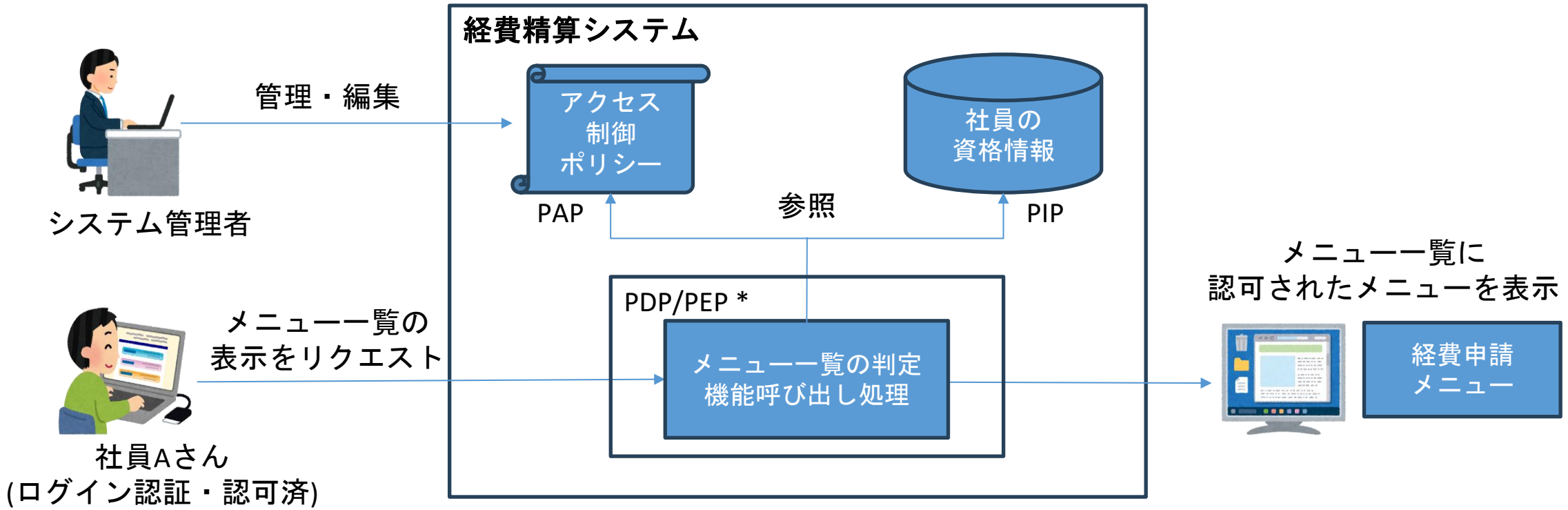
経費支払処理のステップでは、システムログインに関しては、社員であるということが認可の条件となっているが、経費承認メニューの表示、経費の承認といった操作には、財務部所属であるというユーザーの社員区分に応じた制御（RBAC）、および支払処理においては社内ネットワークからのアクセスが条件といった制御（ABAC）が適用されている。

ユースケース③　財務部担当者が支払い処理をする場合の認可のステップ



システム内の認可モデル（構成要素）

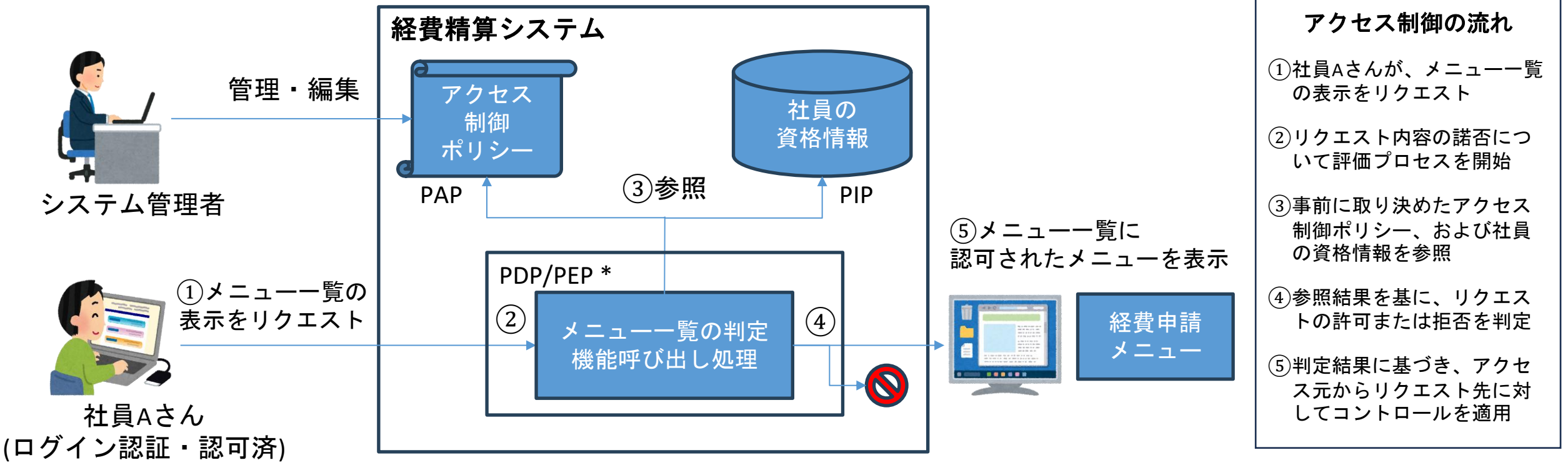
前述の経費精算システムの各種認可制御を実現するために、ユーザーの役職を格納するためのデータベース（社員の資格情報）や、どの機能を使う際にどういった条件を満たす必要があるのかを定めたポリシー（アクセス制御ポリシー）、実際にその機能を提供していいかどうかを判定するための内部判定機能といったシステム構成をすることで、適切な認可制御を行う構成を実現している。以下の図では、経費精算システム利用におけるメニュー一覧表示のステップにフォーカスして記載している。



*システム構成によっては、PDP/PEPが同一コンポーネント上で実装されており、分離されていないケースも存在する

システム内の認可モデル（処理概要）

システム内の認可モデルに関して、アクセス制御の流れに沿っての各コンポーネントの処理概要は以下の形となる。



アクセス制御の流れ

①社員Aさんが、メニュー一覧の表示をリクエスト

②リクエスト内容の諾否について評価プロセスを開始

③事前に取り決めたアクセス制御ポリシー、および社員の資格情報を参照

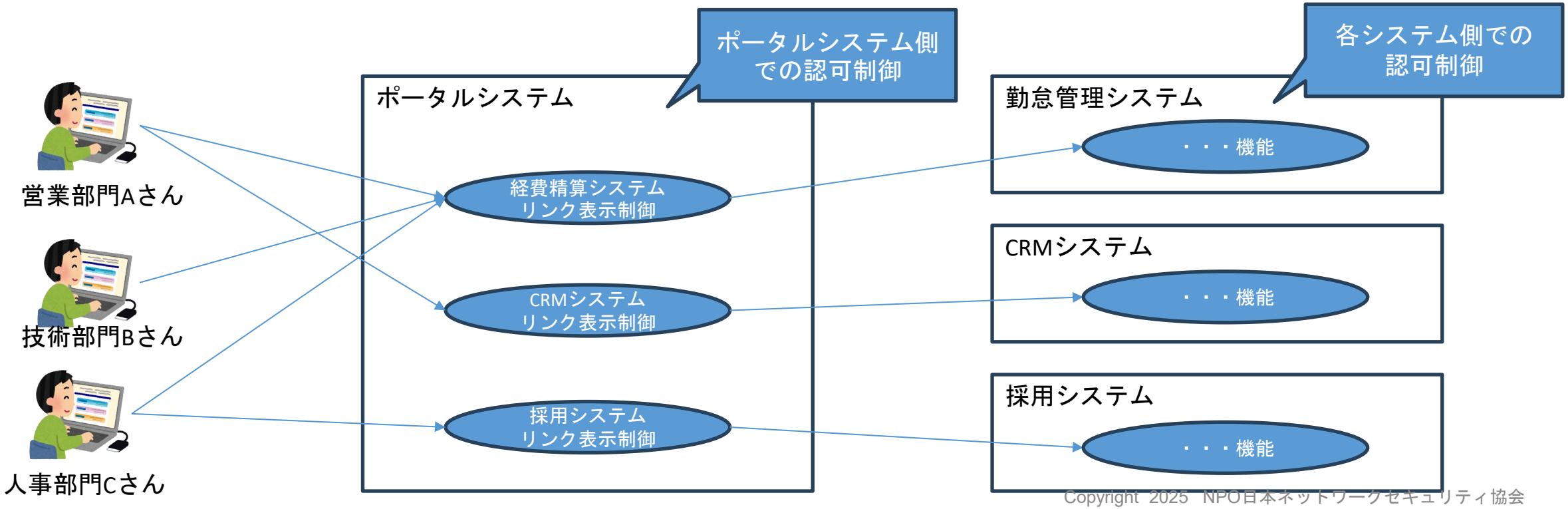
④参照結果を基に、リクエストの許可または拒否を判定

⑤判定結果に基づき、アクセス元からリクエスト先に対してコントロールを適用

複数システムにまたがる認可制御

システムの構成によっては、ポータル機能を担うシステムと各種サービスを提供するシステムが別のシステムとして実装されており、複数システムを横断し利用するといったユースケースも考えられる。

こういったケースにおいても、ポータルシステム側での認可制御や、各システム側での認可制御を考える必要があり、それぞれのシステムにおいても適切な認可を実現する構成を実装することが重要となる。



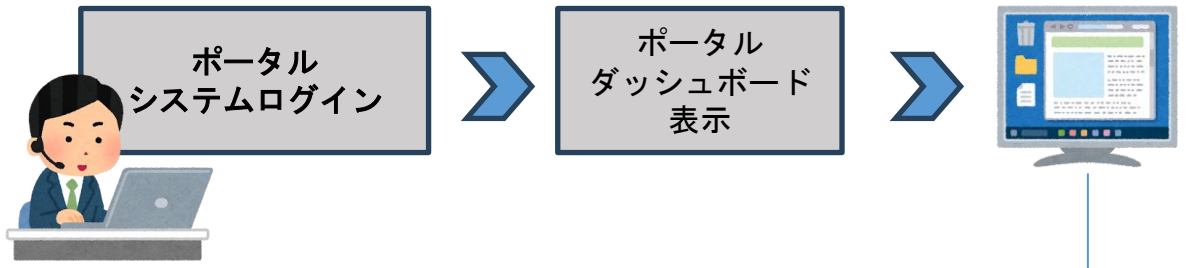
人事部社員が採用システムにアクセスするケースにおける認可制御

前述の複数システムが実装されている環境において、人事部担当者が採用システムにアクセスするケースにおいては、ポータルシステムへのログイン、ダッシュボードから採用システムアクセスの選択、採用システムへのログイン完了といった形で操作処理を実施する。

このステップでは、ポータルシステム側の認可制御として、本人確認やポータルへのアクセス権の検証、採用システムリンクの表示といった制御を実現しており、採用システム側の制御として適切なアクセス権を持つユーザーなのか、そのユーザーがどういった権限を持つのかといった制御を実現している。

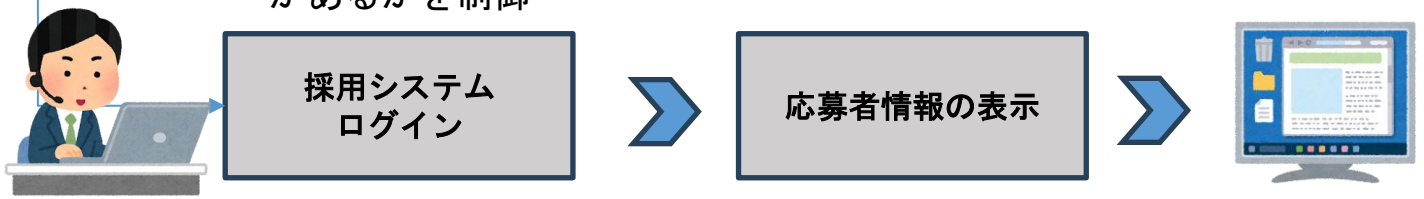
ポータルシステムにおける認可制御

認証・認可により、業務システムに接続する権限があるかを制御



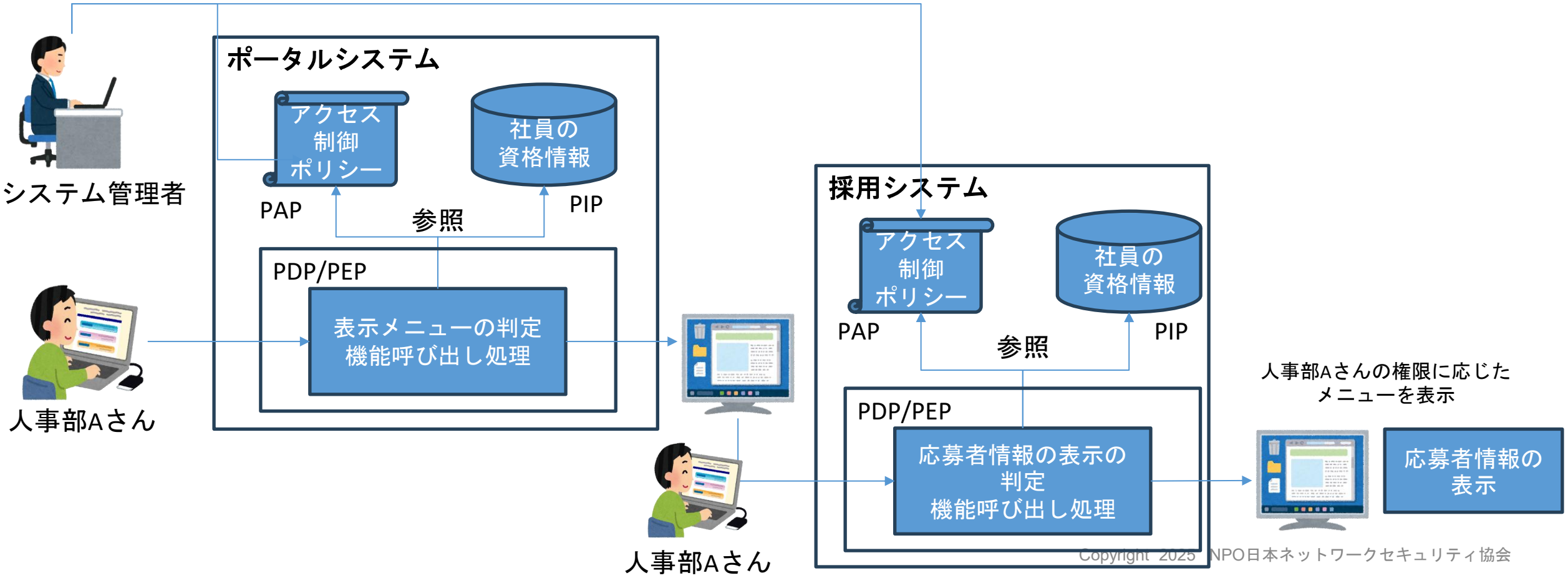
採用システムにおける認可制御

認証・認可により、各アプリケーション上でどんな操作をする権限があるかを制御



複数システムの認可モデル（構成要素）

前述の通り、複数システムにおける認可処理においても、それぞれのシステムにおいて、以下に記載する通りユーザーの役職を格納するためのデータベース（社員の資格情報）や、どの機能を使う際にどういった条件を満たす必要があるのかを定めたポリシー（アクセス制御ポリシー）、実際にその機能を提供していいかどうかを判定するための内部判定機能といったシステム構成をすることで、適切な認可制御を行う構成を実現している。

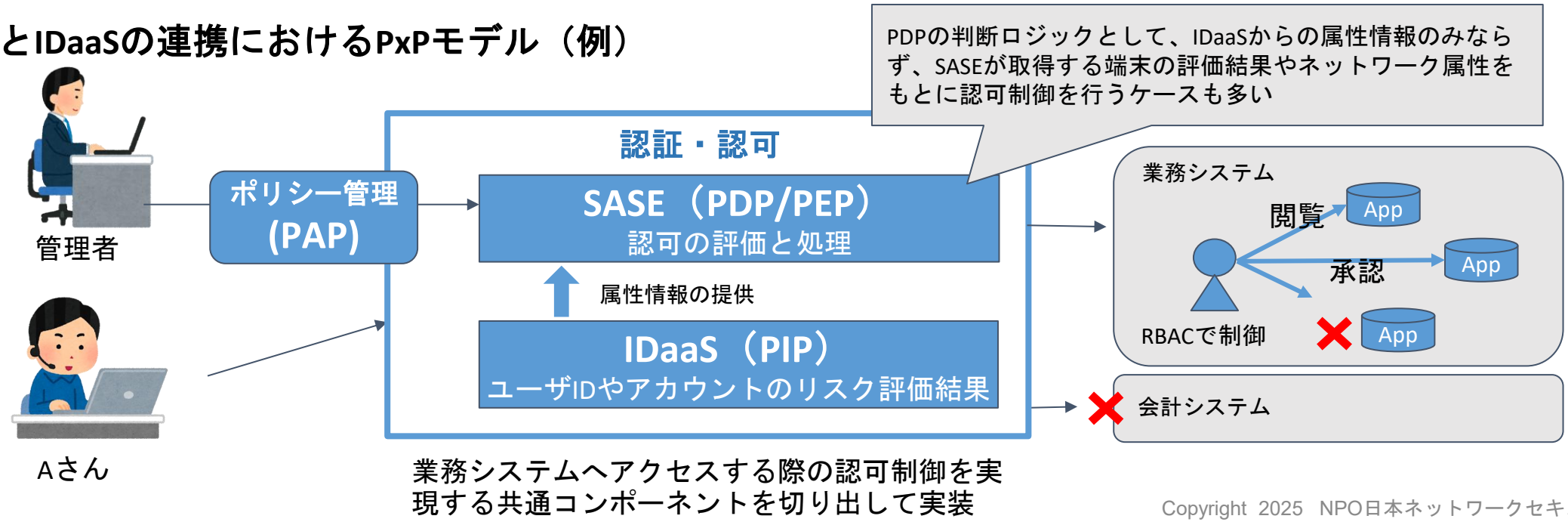


【参考】IDaaSやSASEを活用した場合の認可モデル

システムアクセスへの認可を考慮したとき、この認可制御するコンポーネントを共通化することで、組織ポリシーの一律適用と運用負荷の軽減を期待できる。

以下に、近年利活用が進むIDaaS(Identity as a Service)やSASE(Secure Access Service Edge)についてPxPの論理モデルで整理した例を示す。

■SASEとIDaaSの連携におけるPxPモデル（例）



業務システムへアクセスする際の認可制御を実現する共通コンポーネントを切り出して実装

検討・執筆主要メンバー

検討・執筆主要メンバー（順不同）

佐藤　公理	JNSAサブスクライバ（Silverfort）
山田　達司	JNSAサブスクライバ
相馬　乃亜	デロイト トーマツ サイバー合同会社
星野　亮	株式会社NTTデータ
水原　智広	株式会社ジインズ
亀井　政史	株式会社中電シーティーアイ
水野　洋寿	株式会社中電シーティーアイ
佐藤　篤至	株式会社中電シーティーアイ
宇野　栞	株式会社クエスト
見上　昌成	日本ビジネスシステムズ株式会社
貞弘　崇行	伊藤忠テクノソリューションズ株式会社

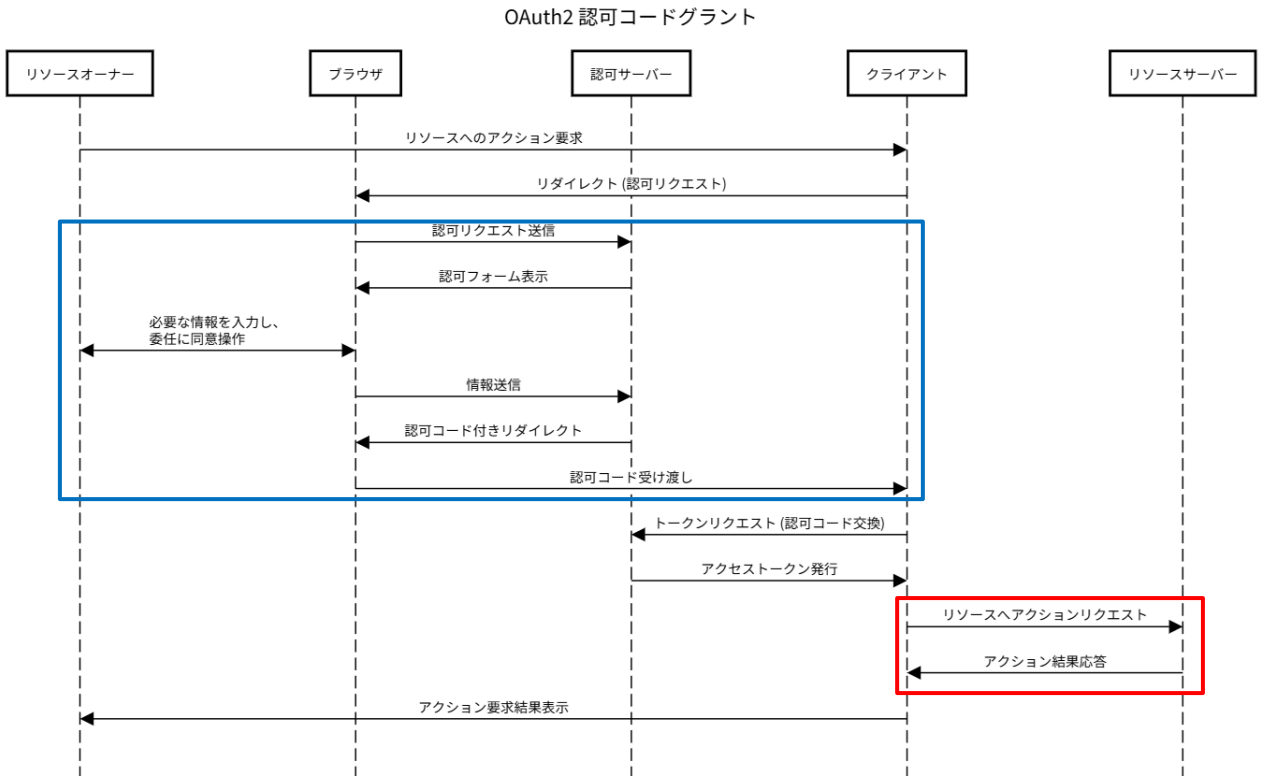
Appendix A. OAuth2での認可との違いは？

OAuth2における認可の定義 1/3

- ✓ OAuth2は「認可フレームワーク」とされる。
- ✓ しかし、OAuth2での「認可」は本資料における認可の定義とは異なり、「委譲すること」という意味を持つ。
  - ✓ Clientとはリソース所有者の「認可」の元でリソース所有者の代わりに保護されたリソースのリクエストを行うアプリケーションのことです。（RFC 6749 1.1 Rolesより。原文は以下）
    - ✓ An application making protected resource requests **on behalf of** the resource owner and with its **authorization**.
  - ✓ RFC 4949においても「主体がリソースへアクセスするために与えられる承認」と定義されている（原文は以下）
    - ✓ 1a. (I) An approval that is granted to a system entity to access a system resource
- ✓ いくつか、OAuth2について説明するサイトでも、「委譲すること」の意味で使われているケースが散見される。（下表赤字部）
  - ✓ 認可とは、**第三者のアプリケーションに、自分のアカウントを用いたWebサービスAPIへのアクセス権限を委譲すること**を言います。
  - ✓ 認証されたユーザーが、どのリソースやデータにアクセスできるかを決めるプロセスです。
  - ✓ 認可（Authorization）は、特定のユーザーがシステム上のリソースにアクセスする権限があるかどうかを確認するプロセス
  - ✓ クライアントはリソースオーナーの**認可を得て、リソースオーナーの代理として保護されたリソースに対するリクエストを行う**役割。

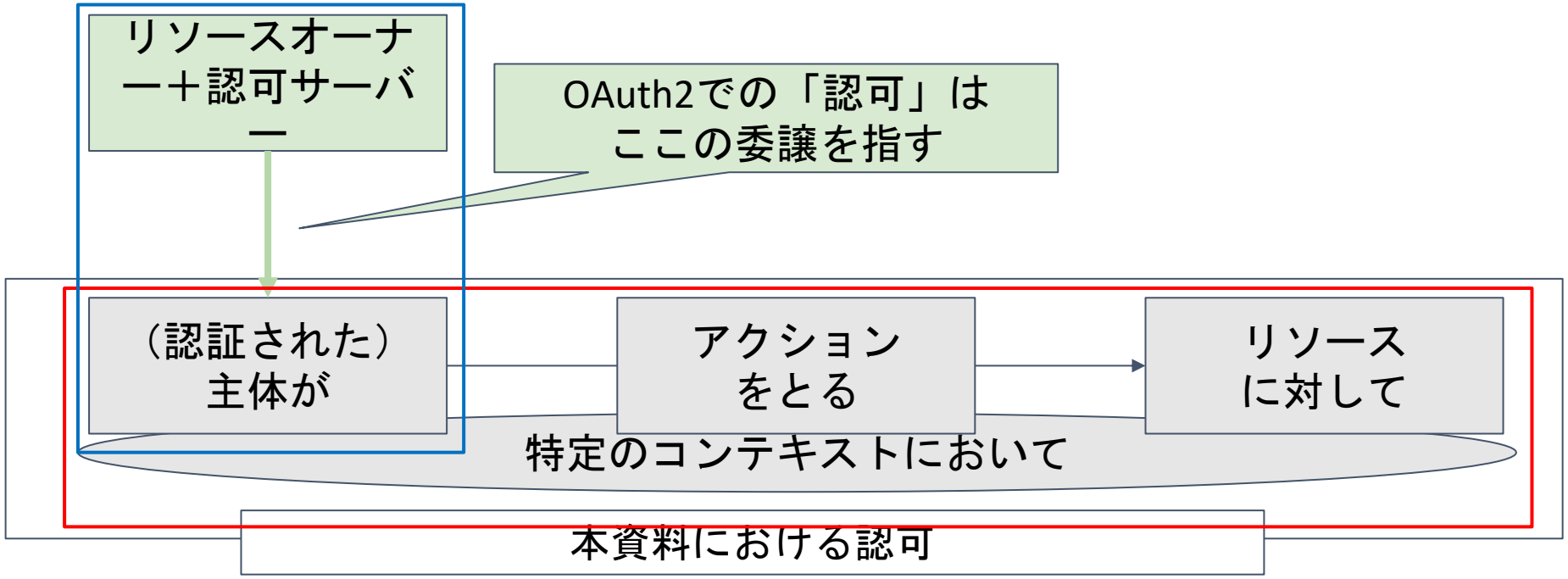
OAuth2における認可の定義 2/3

- ✓ OAuth2の一般的なシーケンス（認可コードフロー）は右図の通り。
  - ✓ クライアント、リソースオーナー、などについてはRFC 6749 1.1 Rolesを参照
- ✓ 本資料における「認可」の定義を踏まえると、リソースに対してアクションを実行する主体はクライアントである。
- ✓ そのため、本資料における「認可」が適用されるのは右図赤枠部となる。
- ✓ 一方、前述の「委譲すること」は右図青枠部で行われている。



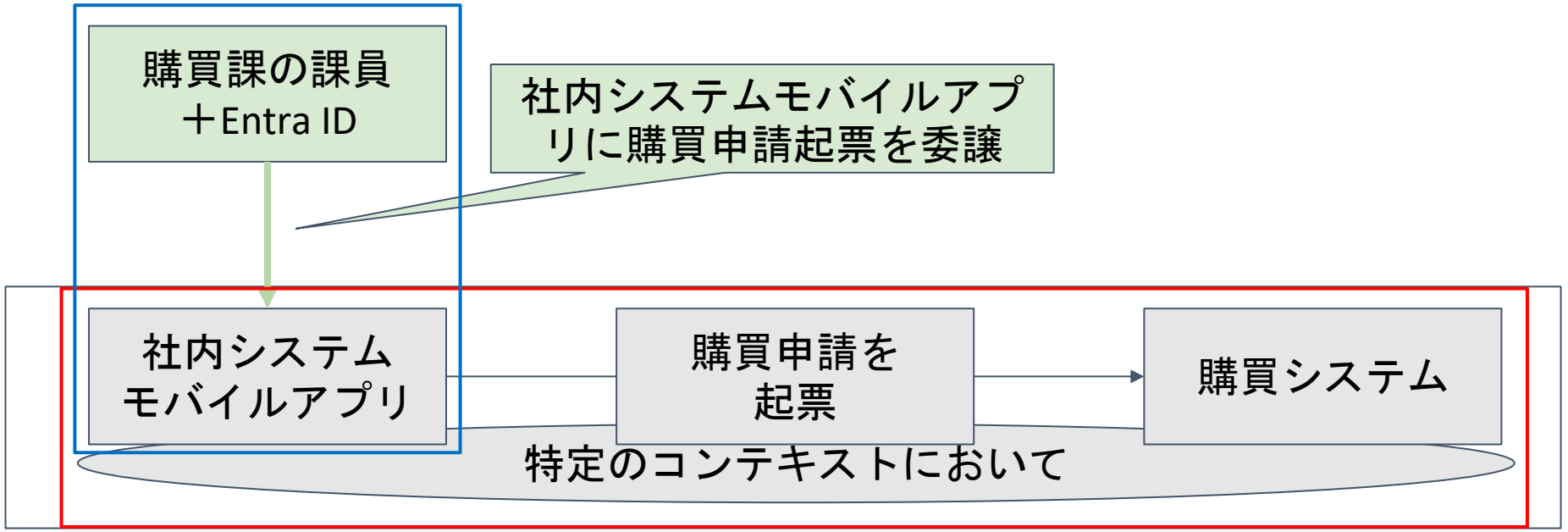
OAuth2における認可の定義 3/3

- ✓ OAuth2での「委譲することを認可」を本資料での認可の定義に当てはめると下図の通りとなる。
  - ✓ 下図における赤枠と青枠はシーケンス上の赤枠と青枠を示す



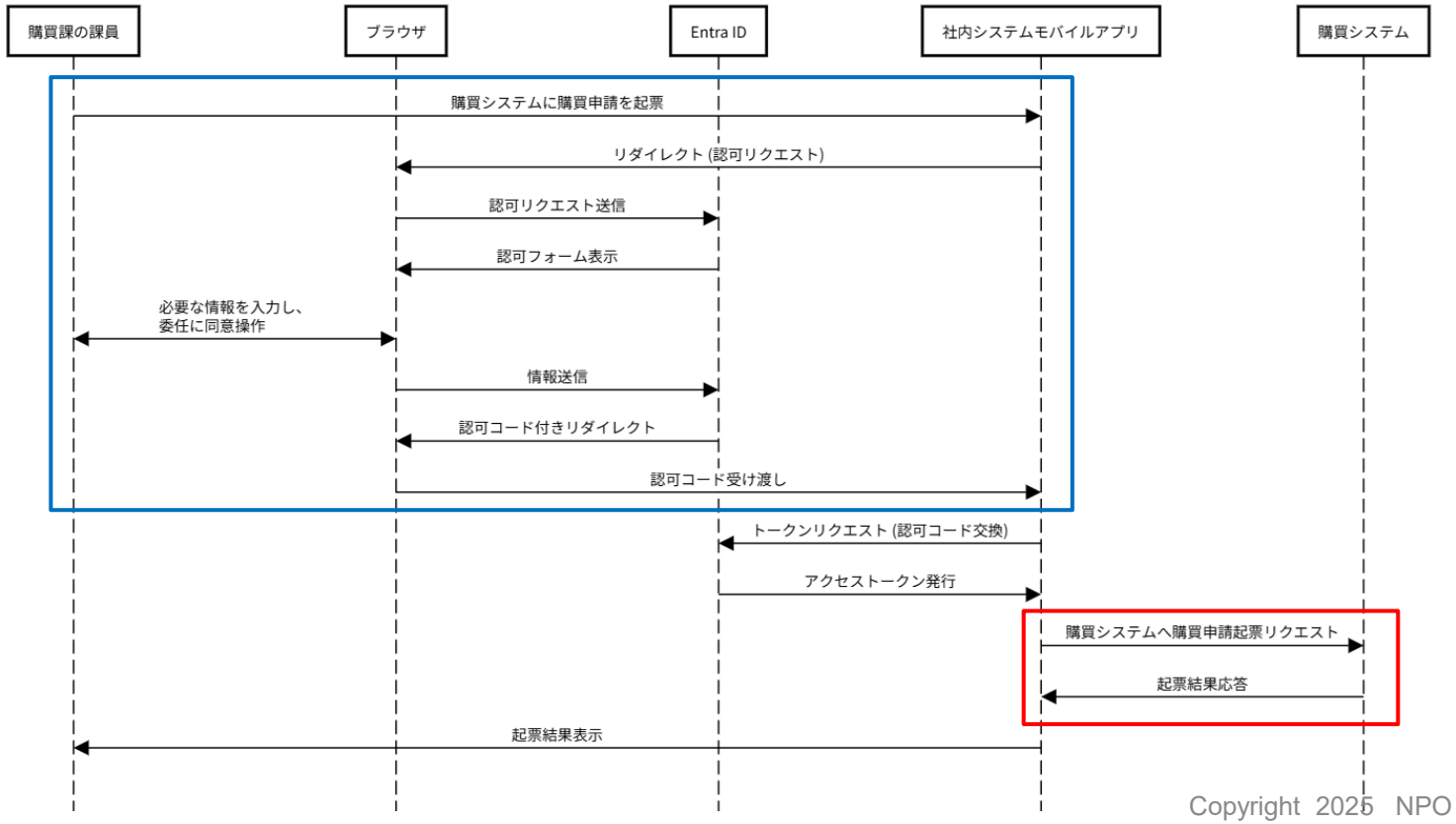
OAuth2における認可の定義（例） 1/2

- ✓ 前頁での図を具体例に当てはめると下図の通りとなる



OAuth2における認可の定義（例） 2/2

- ✓ 前頁での図をシーケンスに当てはめると下図の通りとなる
  - ✓ 本資料における「認可」は赤枠部、OAuth2における「委譲」は青枠部。



Appendix B. ロール管理とは

ロール管理はなぜ必要？　ロール管理今昔　ロール管理の考え方

そもそもロール管理がなぜ必要なのか？

- ✓ 前提
  - ✓ 情報システムを利用するには、**ユーザが利用するアカウント**が当該情報システムに対する**アクセス権**を有している必要がある。

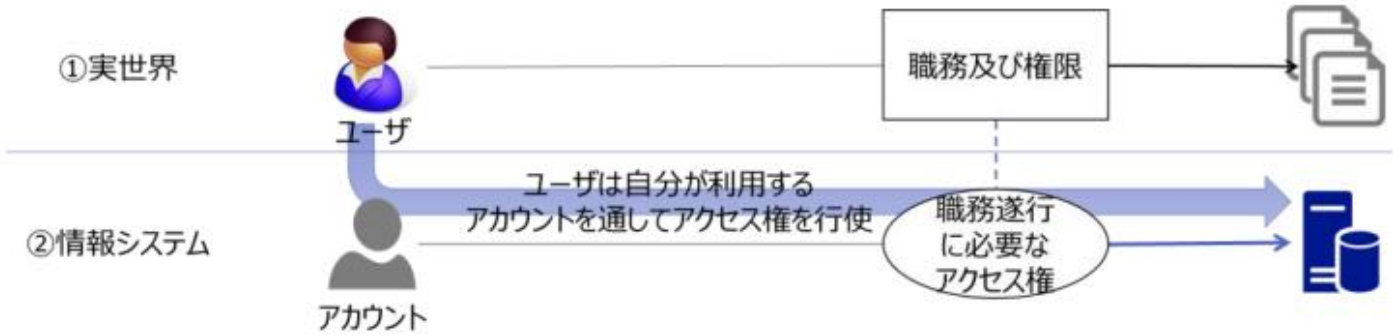


図 1.1　ユーザ・職務の関係とアカウント・アクセス権の関係

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ✓ ロール管理が必要な背景①
  - ✓ ユーザとアクセス権を1対1で管理している場合。ユーザの数×利用するアクセス権分の管理が必要。

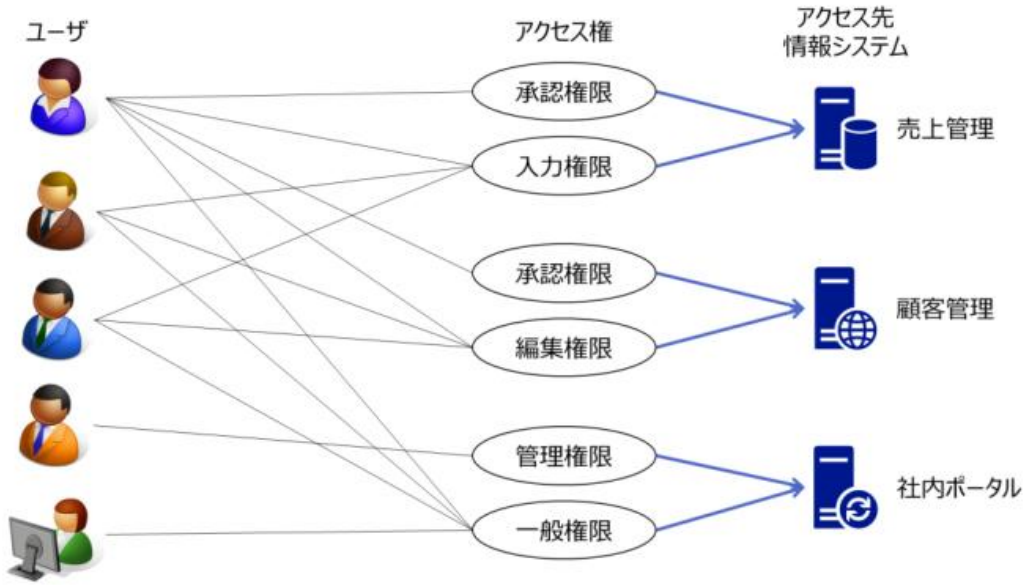


図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

JNSA

- ✓ ロール管理が必要な背景②
  - ✓ ユーザとアクセス権の関係は変化する。

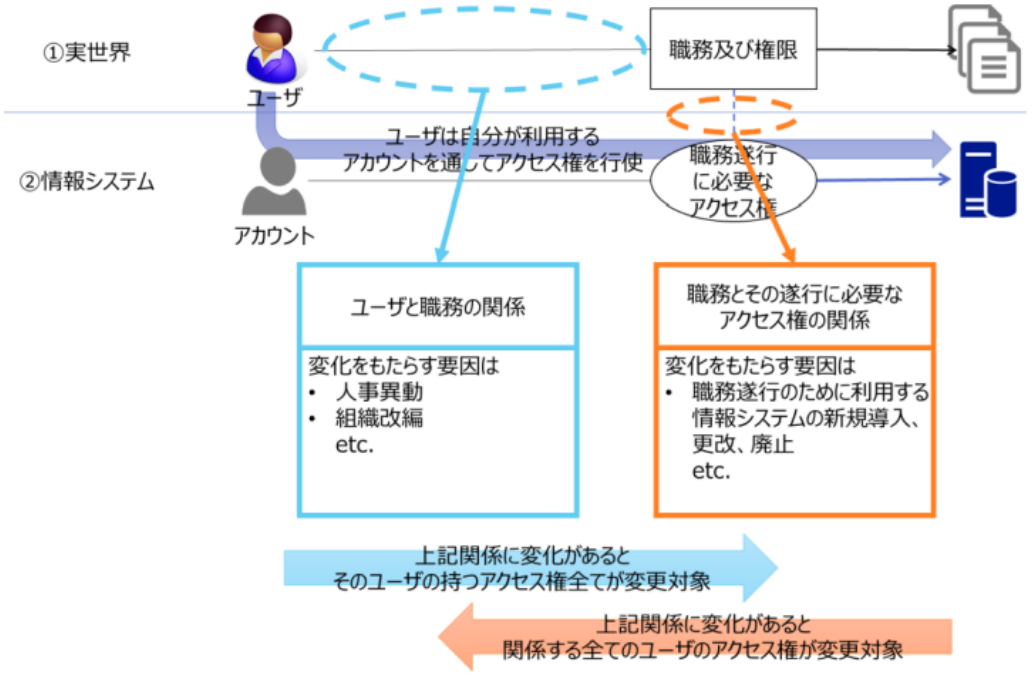


図 1.3 ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介さない場合）

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ✓ ロール管理がないと困る！
  - ✓ ユーザとアクセス権の関係が変化すると。。。
  - ✓ **実現不可能なほど複雑で手間のかかる作業**が発生する。

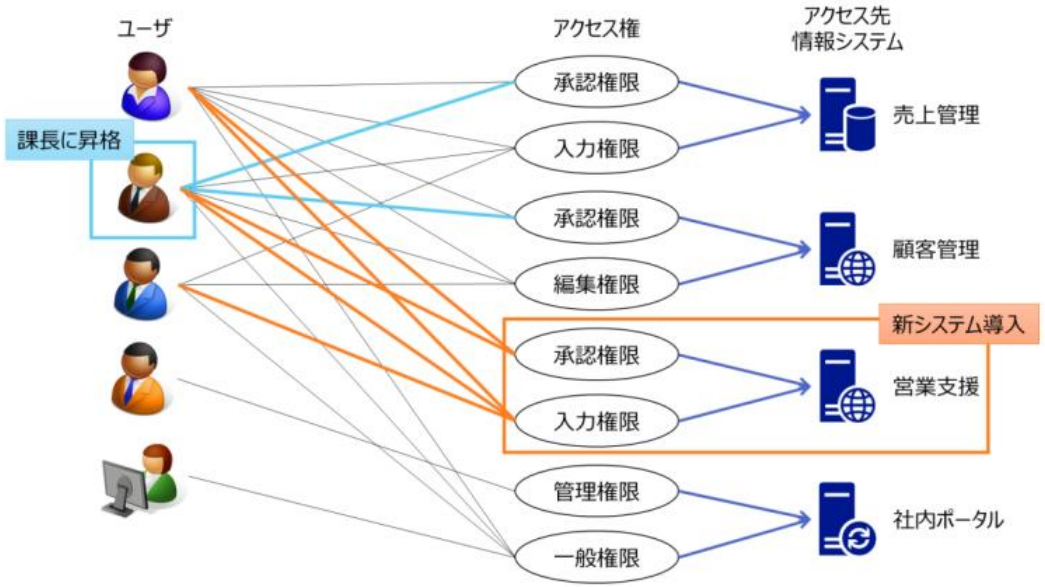


図 1.4　関係に変化が生じた場合のユーザと割り当てるアクセス権の変更箇所

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ✓ ロール登場！
  - ✓ ロールとは！**職務遂行に必要な各種情報システムに対するアクセス権の組み合わせ**
  - ✓ **管理の煩雑さを抑制し、適切な管理を実現！**

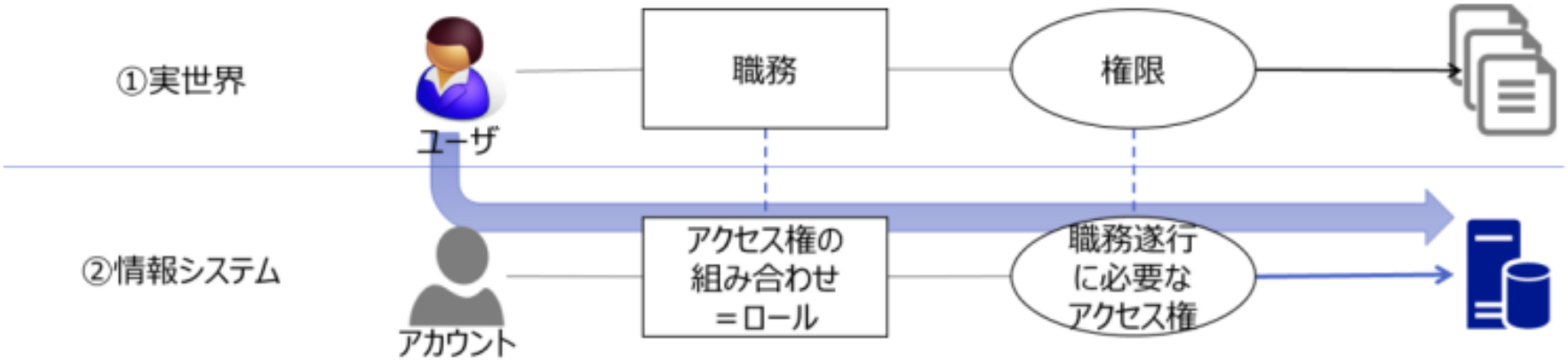


図 1.5　ロールを仲立ちとしたユーザ・職務の関係とアカウント・アクセス権の関係

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

JNSA

✓ ロールを介してアクセス権を割り当てる・管理する。

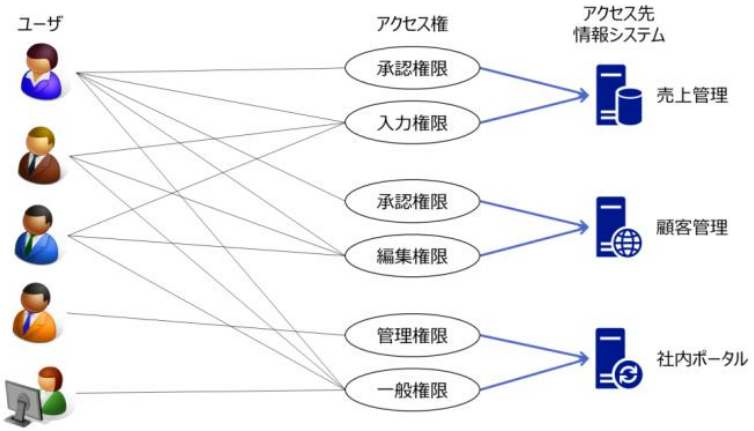


図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態

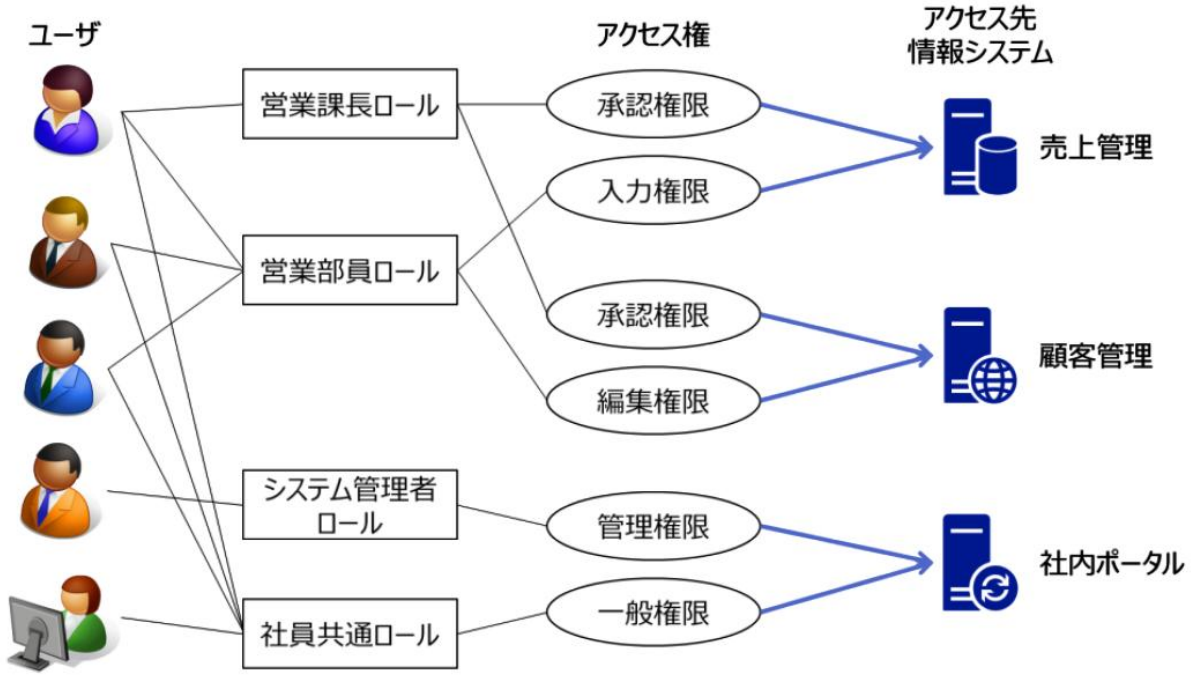


図 1.6　ユーザ（とそのユーザが利用するアカウント）とアクセス権をロール管理している状態

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

JNSA

✓ ロールを介することで**変化の影響範囲が限定される**

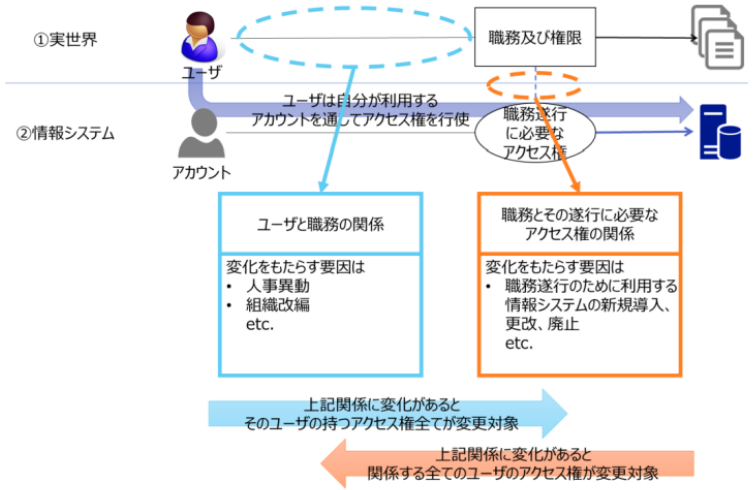


図 1.3　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介さない場合）

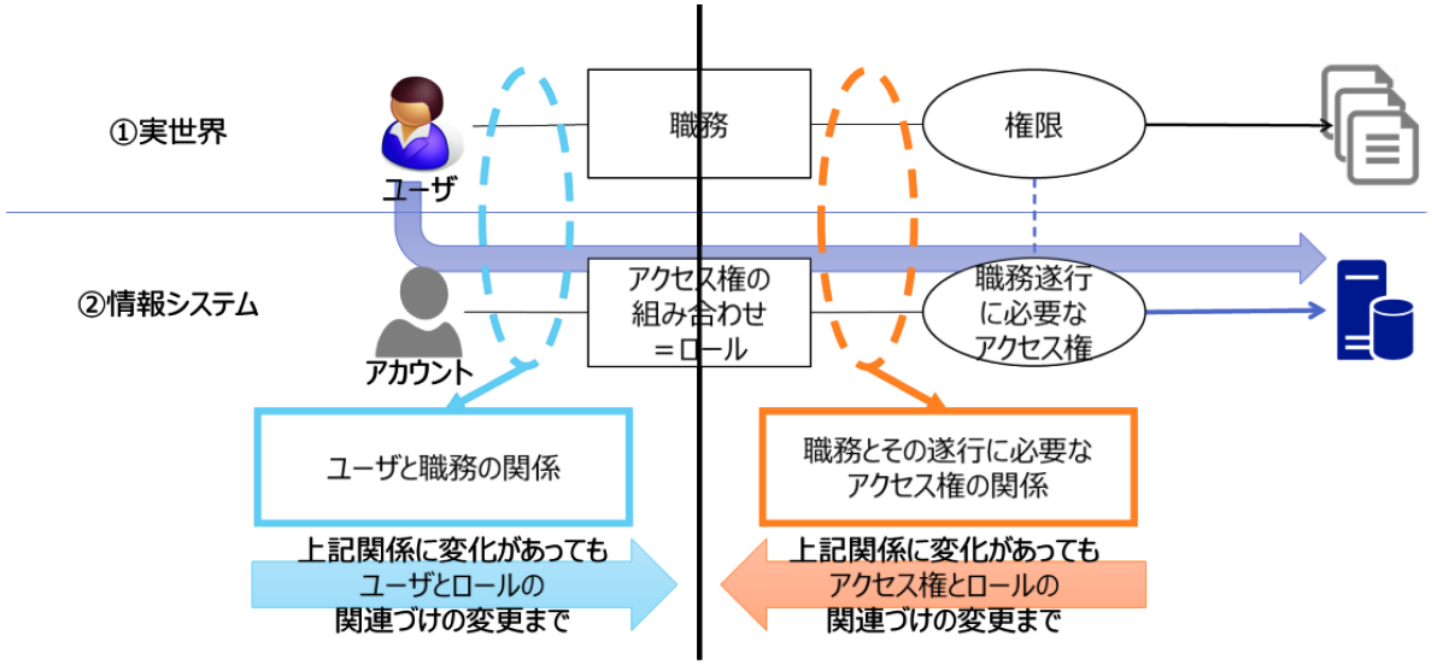


図 1.7　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介す場合）

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

✓ ロールを介することで**変化の影響範囲が限定される！！**

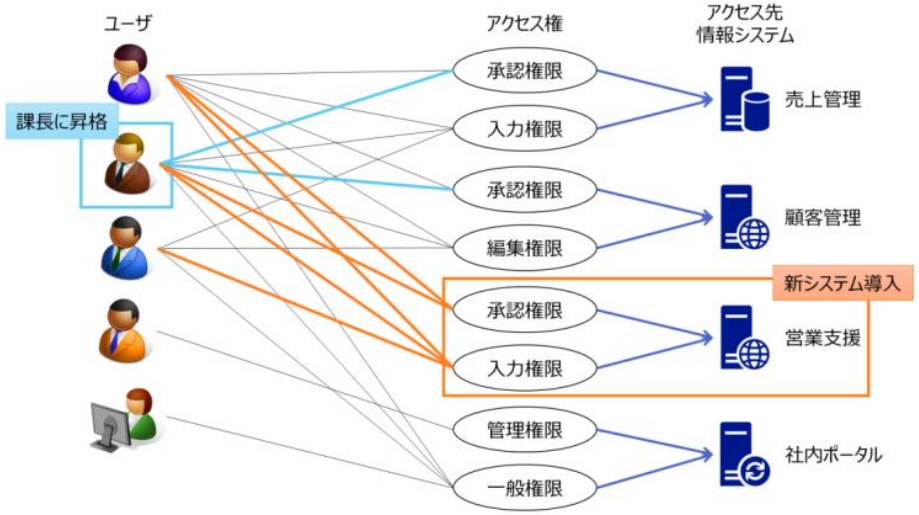


図 1.4　関係に変化が生じた場合のユーザと割り当てるアクセス権の変更箇所

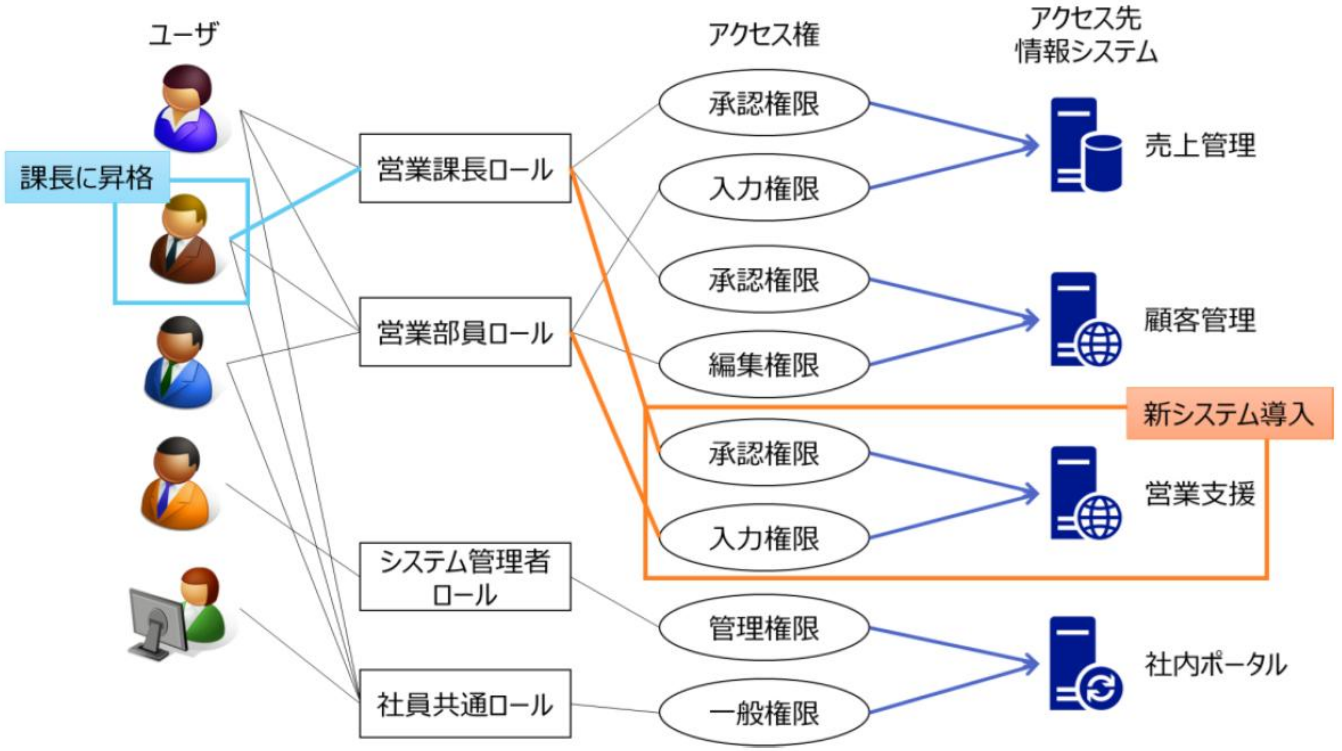


図 1.8　関係に変化が生じた場合のロールに生じる変更箇所

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

アクセス権を効果的・効率的に管理するためにロール管理が必要

ロール管理なしでは、アクセス権の管理は実質的に不可能

ロール管理　今昔

昔

オンプレ
グループマスタ、ロールマスタ、
職務マスタ（社内システム用）

事前に設計。各システムで共有

運用でカバー

ロール定義で自動割当

ADのグループ

今

オンプレ＋クラウド
社内システム用
＋SaaS、PaaS、IaaS

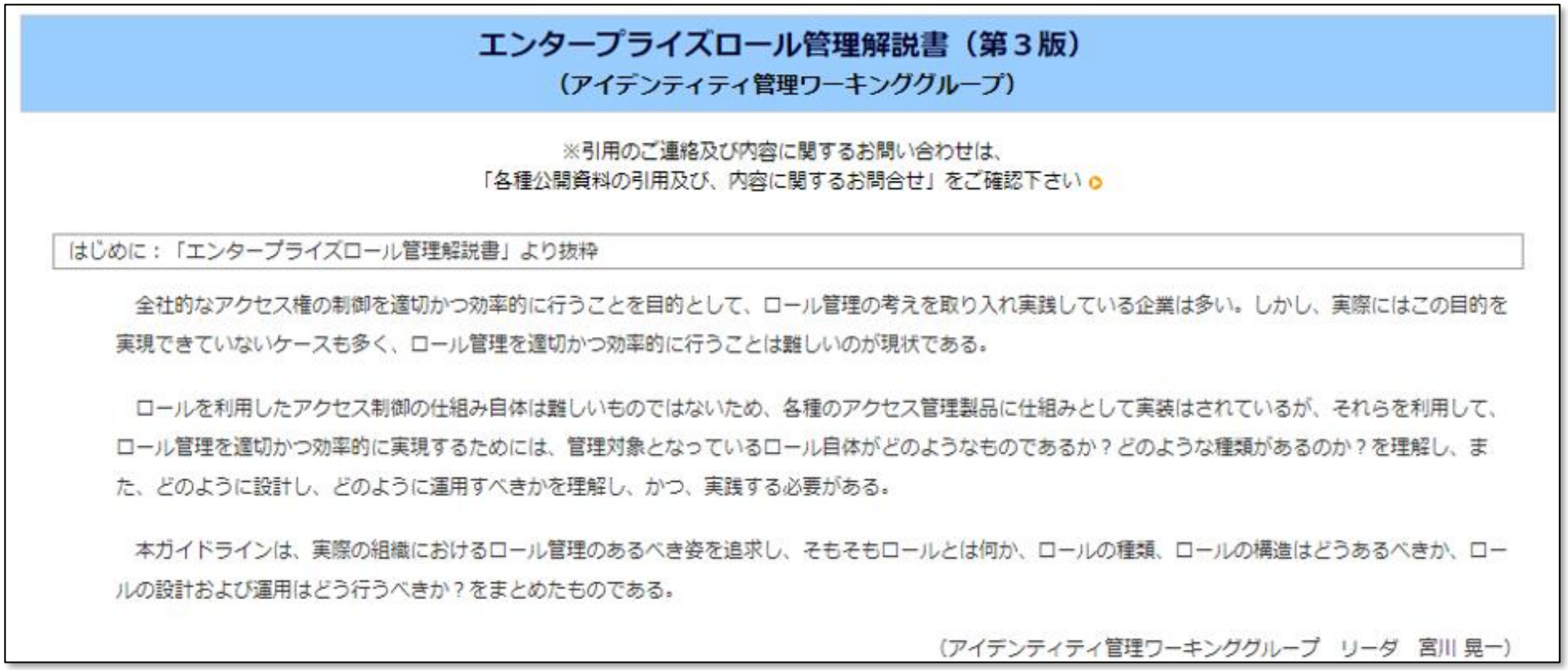
システムに合わせて柔軟に変更、
レビュー

もう運用でカバーできない

自動割当＋アクセス権申請

モデリング、ディスカバリ
アクセス権棚卸

ロール管理　昔から変わらないのは？



エンタープライズロール管理解説書（第３版）
（アイデンティティ管理ワーキンググループ）

※引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご確認下さい

はじめに：「エンタープライズロール管理解説書」より抜粋

全社的なアクセス権の制御を適切かつ効率的に行うことを目的として、ロール管理の考えを取り入れ実践している企業は多い。しかし、実際にはこの目的を実現できていないケースも多く、ロール管理を適切かつ効率的に行うことは難しいのが現状である。

ロールを利用したアクセス制御の仕組み自体は難しいものではないため、各種のアクセス管理製品に仕組みとして実装はされているが、それらを利用して、ロール管理を適切かつ効率的に実現するためには、管理対象となっているロール自体がどのようなものであるか？どのような種類があるのか？を理解し、また、どのように設計し、どのように運用すべきかを理解し、かつ、実践する必要がある。

本ガイドラインは、実際の組織におけるロール管理のあるべき姿を追求し、そもそもロールとは何か、ロールの種類、ロールの構造はどうあるべきか、ロールの設計および運用はどう行うべきか？をまとめたものである。

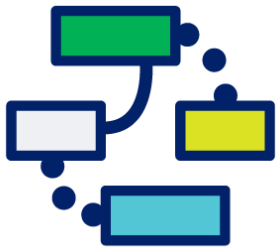
（アイデンティティ管理ワーキンググループ　リーダ　宮川 晃一）

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

「ロール管理の考え」必要性は変わらない

昔から変わらないのは？
ロール管理でもアンチパターン

「似たもの同士ロール」



“十分な検討を行わず、その場その場で必要なロールを作成した。結果、類似のロールが乱立している。

「増殖していくロール」

“ロールの見直し・削除・修正する適切なプロセス・仕組みがない。結果、ロールが増殖・爆発している。”

「メンバ不明ロール」「使用目的不明ロール」

“ロールのメンバがわからない。”
“ロールが使われているかわからない”

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

失敗例（アンチパターン）は変わらない

ロール管理　大きく変わったのは？

設計できるもの（社内システム用のアクセス権）から
最初から決まっている・存在するもの（SaaS やIaaSのアクセス権）へと管理対象が広がり、
より効率的・効果的なロール管理が必要になってきた。

<u>ロール管理自体の深化・進化が必要</u>

クラウド等の複雑なアクセス権への対応
変わらない失敗例を解決する方法（棚卸・分析）